FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

APLICACIÓN DE LA TECNOLOGÍA BLOCKCHAIN EN PROYECTOS DE ONGS

Autor: Ignacio Guitard Maldonado
Director: Ignacio Cervera Conte, SJ

Madrid
Abril, 2018

Ignacio
Guitard
Maldonado

APLICACIÓN DE LA TECNOLOGÍA BLOCKCHAIN EN PROYECTOS DE ONGS

RESUMEN

En el presente trabajo se pretende encontrar cuáles son las maneras posibles de realizar proyectos de ONGs empleando tecnología *blockchain.* Tras una profunda revisión de la literatura, se han determinado cuáles son los principales retos a los que se enfrentan los proyectos del tercer sector y en cuáles *blockchain* puede servir de ayuda. Posteriormente, se han desarrollado cuatro ejemplos de aplicación concreta de la tecnología, mejorando facetas específicas en los tres primeros, y realizando una aplicación global conjunta para el último caso. A continuación, se comentan los posibles problemas que puede haber en la aplicación. Por último, el documento cierra con una conclusión sobre todo lo aprendido de lo estudiado y a qué puntos se han llegado.

Palabras clave: ONG, tercer sector, tecnología, *blockchain,* seguridad, transparencia, aplicación.

ABSTRACT

On the current dissertation, the main objective is to find the different applications that blockchain technology might have for NGO projects. After an extensive review of the existing literature, we have identified the main challenges that non-profit projects are facing and how blockchain might solve them. Additionally, we have developed four application examples, improving specific challenges for the first three, and giving a wider and complete application of the technology for the last one, stating, afterwards, the main setbacks that the implementation may encounter with. The document concludes with the conclusions that summarizes everything learned and the main outstanding points reached.

Keywords: ONG, non-profit segment, technology, blockchain, security, transparency, application

Índice

Índice de figuras

1.- Introducción

1.1- Propósito general de la investigación y contextualización del tema

Lo que se busca con este proyecto es encontrar la posible utilidad que tiene la tecnología *blockchain* en los proyectos de ONGs.

Para poder entender bien a que nos estamos refiriendo, tenemos que pensar en los siguientes elementos:

Por un lado, tenemos un mundo, el de las ONGs, donde se llevan a cabo actividades de carácter lucrativo. ¿Qué significa esto? Significa que están empleando el capital ajeno para favorecer a un determinado sector o para impulsar una idea con las que los inversores se sienten identificados o llamados a colaborar. Como es obvio, es una donación gratuita, sin ánimo de lucro, lo que significa que la donación se realiza bajo la confianza del donante en el receptor. Esta (la confianza), es rota en ocasiones por el que recibe el dinero o, incluso sin tener culpa el que recibe el dinero, aquel que dona empieza a desconfiar sin fundamento, quedando dañada la relación principal entre ONG y receptor. Ahora bien, las organizaciones sin ánimo de lucro no solo tienen este problema; debido a su actividad, necesitan una diligencia muy parecida a las exigidas a las administraciones públicas y su gestión tiene que ser totalmente transparente. En definitiva, y como resumen de este párrafo, el mundo de las donaciones y las entidades que emplean estas necesita de una seguridad y transparencia que puede ser mejorada y reforzada.

Por otro lado, está surgiendo, o más bien se está implantando, la tecnología *blockchain*, de cuyo funcionamiento hablaremos más adelante, siendo su principal ventaja la seguridad de toda la información que aparece en la cadena. Se trata de una tecnología en la que la información queda fijada, tal y como ha sido escrita, y esta no puede ser modificada salvo que sea aceptada por un porcentaje muy alto (más del 90%) de los usuarios; esto permite que todos los partícipes estén al tanto y, además, garantiza la información que se está viendo. Además, sobre la tecnología, cabe decir que existe la opción de un desarrollo por capas de la misma, de manera que alguno de los usuarios no pueda ver información privada de otros usuarios con los que opera la entidad de en

medio (sin dejar de perder la seguridad de la información que se está viendo). En cualquier caso, al margen de estos detalles que hemos puesto para la contextualización, la tecnología *blockchain* parece, a primera vista, una plataforma apropiada sobre la que desarrollar diferentes proyectos como los mencionados arriba.

1.2.- Justificación

Vistos los dos elementos anteriores, queda claro cuál es el objeto de estudio: de qué manera se pueden conjugar ambos elementos para cubrir las carencias del primero. Ya se hablará de esto con posterioridad, en la parte de objetivos, pero lo primero que tenemos que tener en cuenta para abordar este estudio son los problemas que se enfrentan las ONGs a día de hoy; para ello empleamos varios libros en los que describen la problemática de las ONGs, como es el caso la escritora por Moro, L. (2009). Además, hay ya ciertos estudios al respecto que tratan sobre el tema, como el capítulo escrito por Molero, I. en "Blockchain, la revolución industrial de Internet" (Preukschat, 2017). Vistos los puntos clave, pasaremos a analizar y buscar soluciones o formas de compatibilizar ambos elementos y poder dar una respuesta adicional a la problemática.

Dentro de este punto, también considero elemento clave de justificación mi interés personal. Si bien ni tengo ni formo parte de ninguna ONG, sí que he participado en la elaboración de dos proyectos solidarios a gran escala en los últimos 4 años. En el segundo, en el que hoy estoy involucrado, estamos enfrentándonos a una variedad de problemas que quedarían solucionados si se tuviesen herramientas como la aportada por la tecnología *blockchain*. Por tanto, además de la problemática sacada de la literatura, contamos con la experiencia personal que permitirá encontrar nuevos problemas y nuevas formas de afrontar los ya existentes, al saber, en primera persona, de lo que se trata.

1.3.- Objetivos.

Como podemos ver, nos encontramos ante un trabajo de carácter exploratorio y cualitativo.

Sin embargo, este trabajo no pretende solventar la totalidad de los problemas a los que se enfrentan los proyectos solidarios. Por tanto, se tiene que hacer un listado de los

principales problemas, ordenarlos según el criterio de transparencia y seguridad y, finalmente, cubrir con la tecnología *blockchain* los principales.

El primero de los problemas está bastante claro: la financiación de los proyectos. Es necesario dotar de seguridad y transparencia. Seguramente esta parte tenga una función más descriptiva (existen ya proyectos no lucrativos que emplean la plataforma para dar seguridad a las donaciones de los usuarios, como es el caso de KYVA - www.kyva.org -).

Los otros problemas deberán ser abordados, seguramente, desde cero. Aquí primará la función exploratoria y explicativa del proyecto. Con los fallos detectados, se buscará explicar cómo la tecnología *blockchain* los cubre apropiadamente.

1.4.- Metodología.

En cuanto a la metodología del trabajo, tenemos que tener claro que es un estudio cualitativo y, como tal, no podemos estar hablando de muestras poblacionales, medias, medianas, tendencias, correlaciones… En este caso, debido a la limitación de recursos (sobre todo el tiempo), hemos de elegir muy bien cuál va a ser la metodología a seguir.

Emplearemos tres métodos:

1. Revisión de la literatura: Este elemento cobra especial relevancia en el estudio de la tecnología *blockchain*. Cuando planteamos un proyecto solidario, cualquier persona puede, en mayor o menos medida, diseñar una estructura viable de proyecto y sabe cuáles van a ser los puntos más complicados. Sin embargo, en el caso de la tecnología *blockchain*, se trata de algo nuevo y técnico, con el que no se está familiarizado y que exige un esfuerzo de comprensión. Aunque gran parte de lo leído no quedará reflejado en palabras dentro del estudio, sí que servirá para poder estructurar y atacar ordenadamente el trabajo. También se realizará un breve resumen de lo leído para poder contextualizar las partes posteriores.
2. Entrevistas personales con expertos: A continuación, se tendrá que realizar una serie de entrevistas con los especialistas de las diversas materias. Las entrevistas se realizarán con posterioridad a la revisión de la literatura, especialmente en

materia *blockchain*, por la complejidad ya explicada en el punto anterior. Estas entrevistas están a disposición de los profesores correctores del TFG.

3. *Focus group*: Aunque toda la información del proyecto ya está recopilada y se podría realizar el trabajo en su totalidad, un *focus group* permitiría dos cosas: (i) perfilar/mejorar las conclusiones sacadas según la información aportada por los expertos previamente entrevistados individualmente y (ii) realizar una revisión del trabajo.

   Es esencial que el *focus group* se realice al final del proyecto, para poder mantener un orden y no abarcar más de lo posible. Una crítica razonable sería la de emplear este método al comienzo, sin embargo, esto no parece viable por la ya mencionada escasez de recursos.

1.5.- Personas entrevistadas

Ignacio López del Moral

Ignacio López del Moral es abogado español, que cursó la licenciatura de Derecho (premio de excelencia) y ADE en el Colegio Universitario de Estudios Financieros (CUNEF) y, tras una preparación como notario público, empezó a trabajar en la consultora Everis como consultor de negocio y abogado *blockchain* en el departamento digital. Paralelamente, profundizó en materias de cumplimiento de pagos y pasó a formar parte de Blockchain España (de la que actualmente sigue formando parte) como nodo legal. Recientemente ha abandonado su puesto en Everis para empezar en la empresa internacional UST Global.

Daniel Díez García

Es uno de los autores del libro "*blockchain:* la revolución industrial del internet". Especialistas en aspectos financieros y *blockchain*, Daniel fue director de estrategia y desarrollo de negocio de Bit2Me, la primera aplicación que conecto a la red el cajero tradicional. Fundó también la primera consultora española relacionada con *blockchain* y, posteriormente, fue el responsable de *blockchain* EMEA en Everis, donde trabajó de la mano con Ignacio López del Moral. Además, forma parte de numerosas instituciones de educación, donde tiene un rol activo en hacer llegar el *blockchain* a los estudiantes. Hoy trabaja en UST Global como encargado de *blockchain* a nivel internacional.

David Contreras Bárcena

Doctorado en ingeniería informática por la Universidad Pontificia de Comillas, lleva 27 años de profesor de la escuela técnica de ingenieros de ICAI y, desde hace casi dos años, es director del departamento de telemática y computación. También ha participado en otros programas como en la *Loyola University of Chicago* de profesor invitado.

Israel Alonso Martínez

Doctorado en ingeniería informática por la Universidad Pontificia de Comillas. En 1998 comenzó su docencia en ICAI impartiendo clases en los títulos de ingeniería informática e ingeniería técnica informática.

José Luis Gahete Díaz

Doctor en ingeniería informática por la Universidad Pontificia de Comillas, lleva 24 años de profesor de la escuela técnica de ingenieros de ICAI. Ha sido jefe de estudios de los títulos de Ingeniería técnica e Ingeniería en informática y director del departamento de sistemas informáticos de ICAI. Además, fue profesor invitado durante el curso académico 2015-16 en *Loyola University of Chicago.*

Manuel Hurtado

Realizó sus estudios en el Massachusetts Institute of Technology (MIT) en Fintech. Está inmerso en varías iniciativas relacionadas con el mundo de las tecnologías, entre las que se destacan: CEO de Global Technology Knowledge, principal en H. Investments, miembro de la mesa de directores de itwillbe.org y consejero asesor de la fundación para la innovación financiera y la economía digital. Además, es presidente fundador de la ONG Common Good Chain, que pretende llevar la *blockchain* al mundo de las entidades sin ánimo de lucro y las actividades del tercer sector.

Alfonso Masoliver Sagardoy

Alfonso es estudiante de marketing y publicidad de la universidad San Pablo Ceu que quiere dedicar su futuro profesional al mundo del tercer sector. Cabe destacar larga participación en proyectos solidarios tanto en África como América, habiendo estado en proyectos en Costa de Marfil (un mes), Haití (dos meses) y Guinea-Bissau (dos meses y

medio). De la mano de la ONG con la que fue a Guinea-Bissau (Aida.org), Alfonso está liderando un proyecto para la misma llamado Proyecto 41.

2.- Tecnología *blockchain*

Analizados los motivos, metodología y demás aspectos iniciales, se procede a analizar la primera pata clave del estudio: la tecnología *blockchain*, cuyos rasgos principales, entre otros de los que hablaremos más adelante, son la seguridad y la transparencia.

Para comenzar, vamos a utilizar las palabras de Alex Preukschat e Íñigo Molero Manglano (Preukschat 2017, 15) que dicen: "el único límite que conoce la *blockchain* es la propia imaginación del ser humano". Estas palabras tienen una fuerte influencia en el presente trabajo ya que como vamos a ir viendo, habrá medidas que se puedan llevar a cabo inmediatamente (como por ejemplo sería crear una plataforma de transacciones internacionales dentro de la ONG para una gestión más eficiente del dinero), otras que aún no se han desarrollado aún, pero podrían realizarse gracias a los principios de la tecnología (ejemplo hipotético: crear un modelo de gestión empleando la *blockchain*) y otras soluciones que, aun siendo ya existentes, pueden chocar con el contexto legal (en el ejemplo puesto sobre las transacciones internacionales ¿Se podría realizar las transacciones de manera interna al margen de los requisitos legales para la transmisión del dinero internacionalmente?)

2.1.- Descripción técnica

Definición

El origen de la *blockchain* tal y como se conoce hoy, está basado en la criptomoneda *Bitcoin*. Sin embargo, a pesar de que su aparición haya sido en el año 2008 tras la publicación del artículo "*Bitcoin: a peer-to-peer electronic cash sistem*[1]*"* (Nakamoto, 2008), ya en años anteriores se buscó con ahínco un protocolo que, junto con la criptografía, solucionase el problema del doble gasto, la fiabilidad y la transparencia, como fue el caso de David Chaum, fundador de DigiCash, o el artículo de uno de los socios de la misma, Nick Szabo: "*Imagine the ideal protocol. It would have the most*

[1] Traducción: "Bitcoin: un sistema monetario de usuario a usuario." (Traducción propia)

trustworthy third party imaginable – a diety who is on everybody's side. All the parties would send their inputs to God. God would reliably determine the results and return the outputs. God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output."[2] (Szabo, 1997).

En cualquier caso, de esta búsqueda anterior a la criptomoneda Bitcoin, podemos sacar una primera definición: *blockchain* es un protocolo fiable que, por medio de herramientas como la criptografía, consigue dotar a toda la información que forma parte de la misma de seguridad y transparencia.

Continuando con la línea temporal, en el año 2008, Satoshi Nakamoto publica el mencionado artículo en el que establece las reglas de funcionamiento de Bitcoin, donde se encuentra por primera vez el nombre de *blockchain*. En las conclusiones del escrito (punto 12) se realiza una definición más a fondo del protocolo fiable mencionado con anterioridad: una red entre iguales (*peer to peer*) que va acumulando un trazado de las diferentes actividades realizadas, aprobadas por el método de prueba del trabajo (del que hablaremos más adelante), donde habría que tener el control de la mayoría de los usuarios para poder modificar la actividad realizada en el mismo y donde la criptografía tiene un papel fundamental.

Sobre los dos puntos anteriores podemos cerrar el concepto de *blockchain* que utilizaremos el resto del trabajo: Se entiende por *blockchain* como ese protocolo fiable entre iguales donde todas las personas que intervienen en el mismo son fedatarios de las actividades realizadas por los demás y ratificándose las mismas por medio de diferentes métodos de prueba.

---

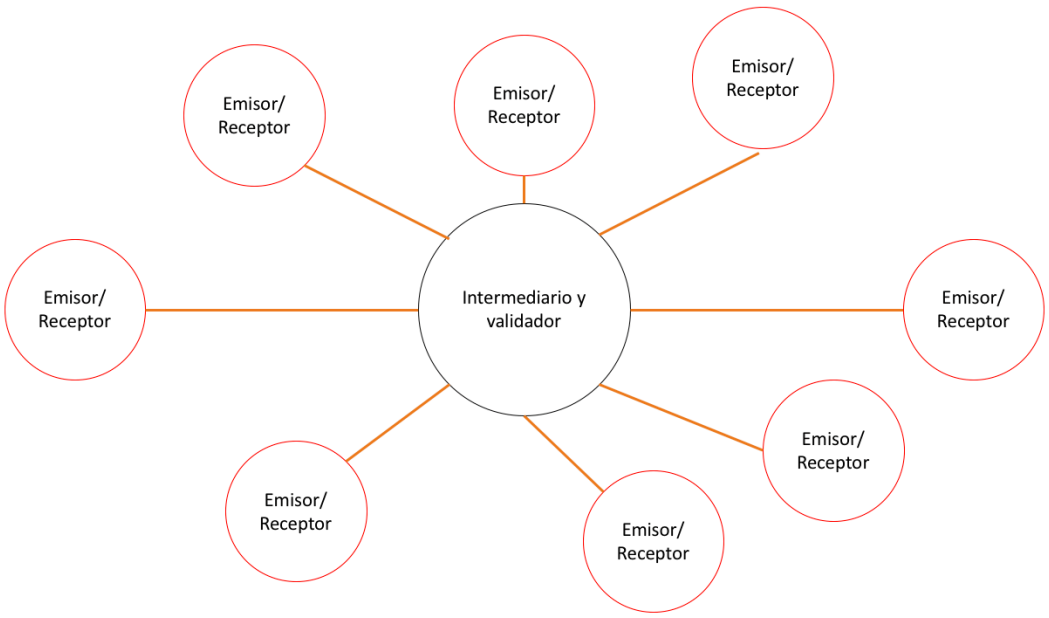
[2] Traducción: "Imagina el protocolo ideal. Debería tener la tercera parte más fiable jamás imaginada, una deidad que está del lado de todos. Todas las partes enviarían su información a dios. Dios determinaría confiadamente el resultado y daría un *output.* Dios sería lo último en secreto de confesión, ninguna de las partes podría aprender algo de otra más allá que lo que ella misma informa y obtiene directamente" (traducción propia).

Como Julio Faura, responsable de *blockchain* en el Banco Santander y miembro de la junta de Alastria, dijo en una charla en enero de 2018: "Blockchain permite establecer una verdad única entre los diferentes usuarios de la red sin la necesidad de intermediarios"

DLT

Ahora bien, la *blockchain* que acabamos de definir no se podría implementar sin el concepto de *DLT* o *Distributed Ledger Techonology*[3]. Al comienzo de la era tecnológica toda comunicación o transmisión de información se tenía que realizar por medio de una entidad central o intermediario, que canalizaba todas las operaciones y las comprobaba. El ejemplo clásico es el caso de los bancos (véase figura I).

FIGURA I: ESTRUCTURA DE LA RED CON INTERMEDIARIO CENTRAL



Fuente: elaboración propia

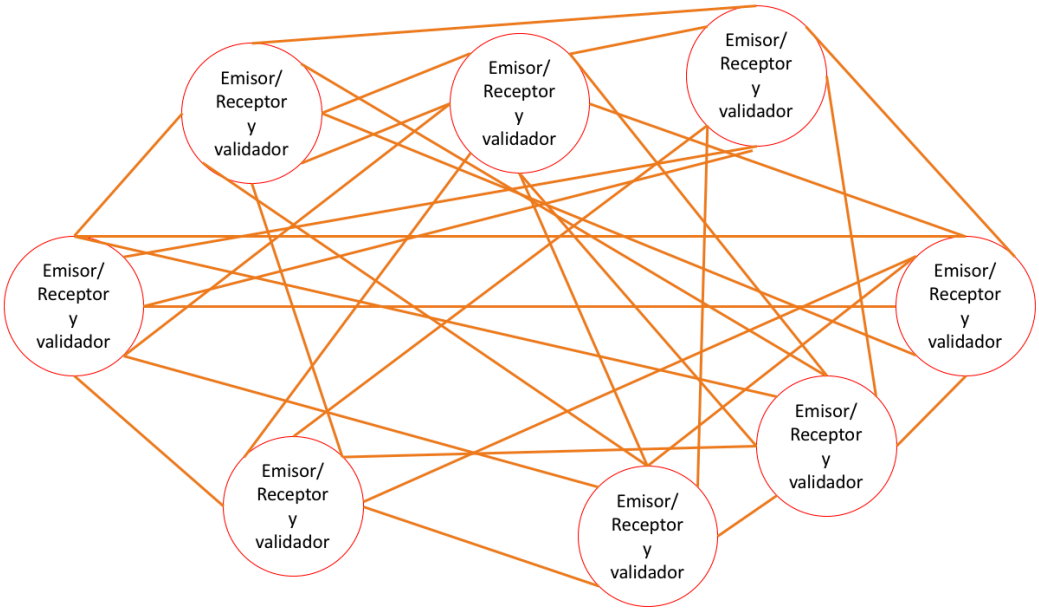
Esto generaba muchos problemas como podía ser información diferente entre la emitida y la recibida, intercepción de lo comunicado, vicio del intermediario…, y uno muy grave: ¿Qué pasaba si el intermediario validador "se caía"? Que el sistema entero

[3] Traducción: "Tecnología de capas distribuidas." (Traducción propia)

podía caer. Una posible solución era crear más nodos validadores, es decir, más intermediarios, de tal manera que en caso de caer uno quedasen los otros. Sin embargo, sigue existiendo el mismo problema; es relativamente sencillo que caigan los pilares y con ellas el sistema en si.

Es precisamente la idea *DLT* de una capa de usuarios distribuido lo que terminaría con un proceso no distribuido que puede fallar y dejar la totalidad del sistema colapsado. De esta manera, si uno cae, los otros se mantienen y, con ellos, el sistema. Es cierto que el sistema podría caer en el caso de que todos los nodos fallen, pero la complejidad es mucho mayor; además, si el sistema distribuido se fundamenta en el protocolo fiable definido anteriormente y explicado a continuación, sería aún más seguro y fiable. Los nodos intermediarios desaparecen y los usuarios se encargan de sustentar el sistema, de manera que no dependen de ningún tercero, sino que son ellos mismos los que tienen que transmitir la información o permiten que pase a través de ellos (véase figura II).

FIGURA II: ESTRUCTURA DE LA RED CON CAPAS DISTRIBUIDAS (DLT)



Fuente: Elaboración propia

Un problema de que la información pase por todos los nodos es mantener la confidencialidad. Este problema encuentra solución con la criptografía, de la que se habla a continuación.

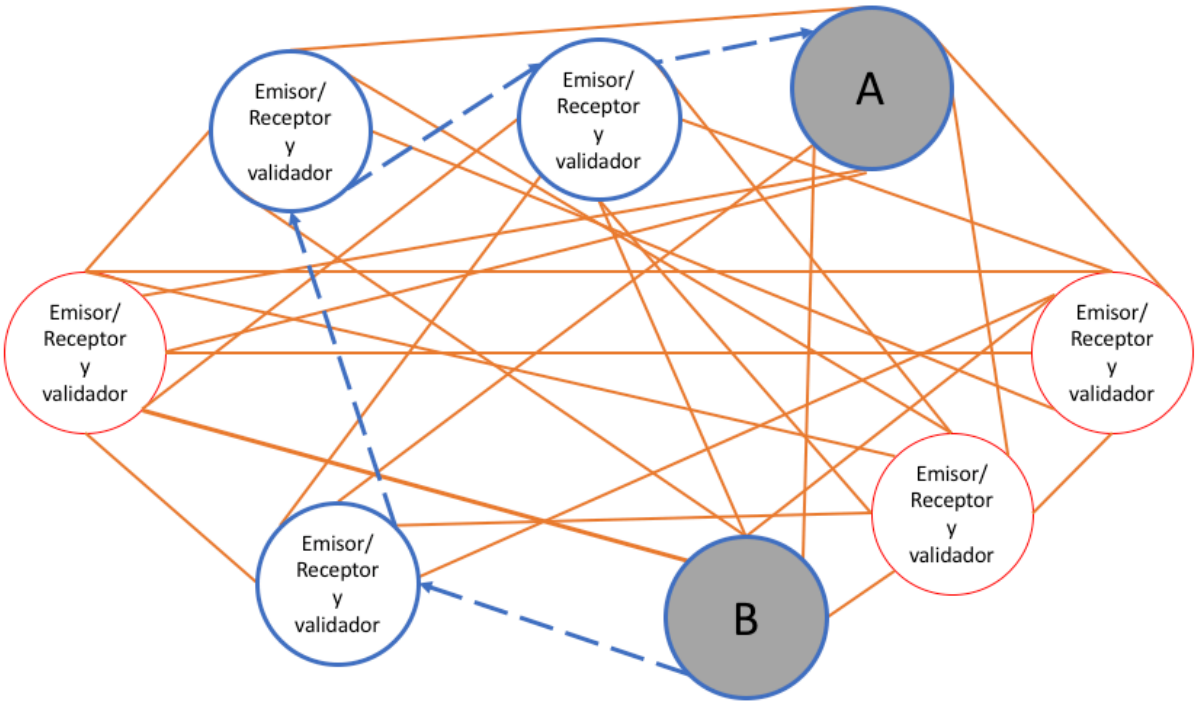
La criptografía

De igual manera que es necesario entender la *DLT* para estudiar la *blockchain,* lo mismo ocurre con la criptografía: "No es posible conocer el funcionamiento de la tecnología *blockchain* sin una aproximación a uno de sus elementos básicos, la criptografía. A partir de él se descubre todo su potencial en campos tan diversos de la vida como el industrial, el económico o el de la información.

La criptografía es el arte de transformar un mensaje legible en otro ilegible. A este proceso se le llamado 'cifrado', mientras que el contrario, la recomposición del mensaje en un formato legible, es el 'descifrado'" (Núñez Miller, 2017, 203).

La criptografía permite que los mensajes y la información recogida en la cadena de bloques no sea legible más que por el receptor del mensaje. En la figura III inferior podemos ver cómo un mensaje que emite B para llegar A tiene que pasar por varios nodos.

FIGURA III: TRANSMISIÓN DE UN MENSAJE EN UNA RED DISTRIBUIDA



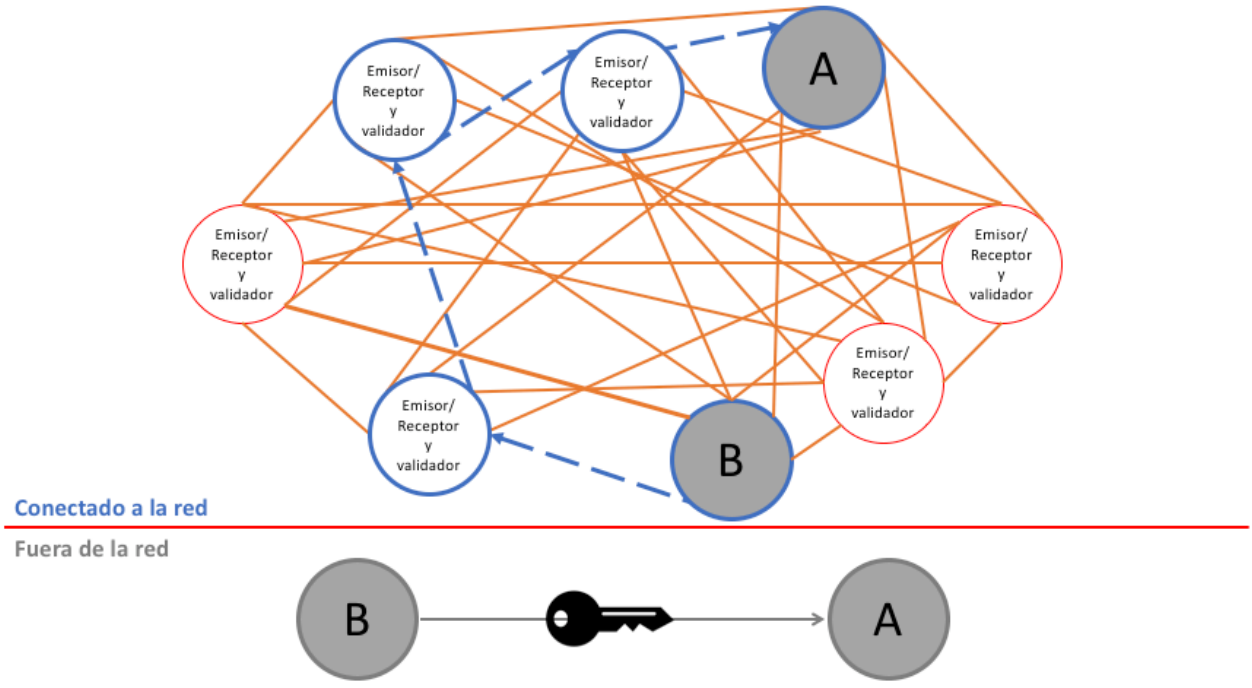
Fuente: Elaboración propia

El mensaje no sigue una línea directa, si no que utiliza otros tres usuarios para llegar al receptor y, además, puede ser visto por la totalidad de la red. Aunque lo que se busca

con la cadena de bloques, entre otras cosas, es la transparencia de las actividades, esta no tiene porqué ser de conocimiento de toda la gente; simplemente tiene que estar a la vista de todo el mundo los movimientos realizados y saber que en caso de que la realidad "mute" por un artificio, el error se detectaría con cierta facilidad. Por tanto, hay que proteger el mensaje y ello implica que solo las personas involucradas puedan abrirlo.

El método habitual, explicó José Luis Gahete Díaz en la entrevista realizada, era el siguiente: "Generalmente el mensaje era relativamente fácil de encriptar y que la gente no lo entendiese. Por tanto, el emisor – B en el ejemplo - cifra el mensaje y crea una clave (llave) que sirve para descifrar lo cifrado; posteriormente A recibía el mensaje y la clave del mismo y así podía ver qué era lo que contenía. El problema es obvio, la única manera de pasar la clave sin que pudiese ser interceptada era fuera de la red; había que hacerlo en persona o estar en una red privada sin acceso al exterior para que nadie entrase." Esto es lo que se denomina criptografía simétrica; realizar una transacción segura implicaba un esfuerzo adicional bastante costoso y que favorecía la presencia de intermediarios de confianza que gestionasen estos problemas. En un sistema distribuido, la situación sería como muestra la figura IV.

FIGURA IV: EMPLEO DE LA CRIPTOGRAFÍA SIMÉTRICA PARA LA TRANSMISIÓN DE UN MENSAJE

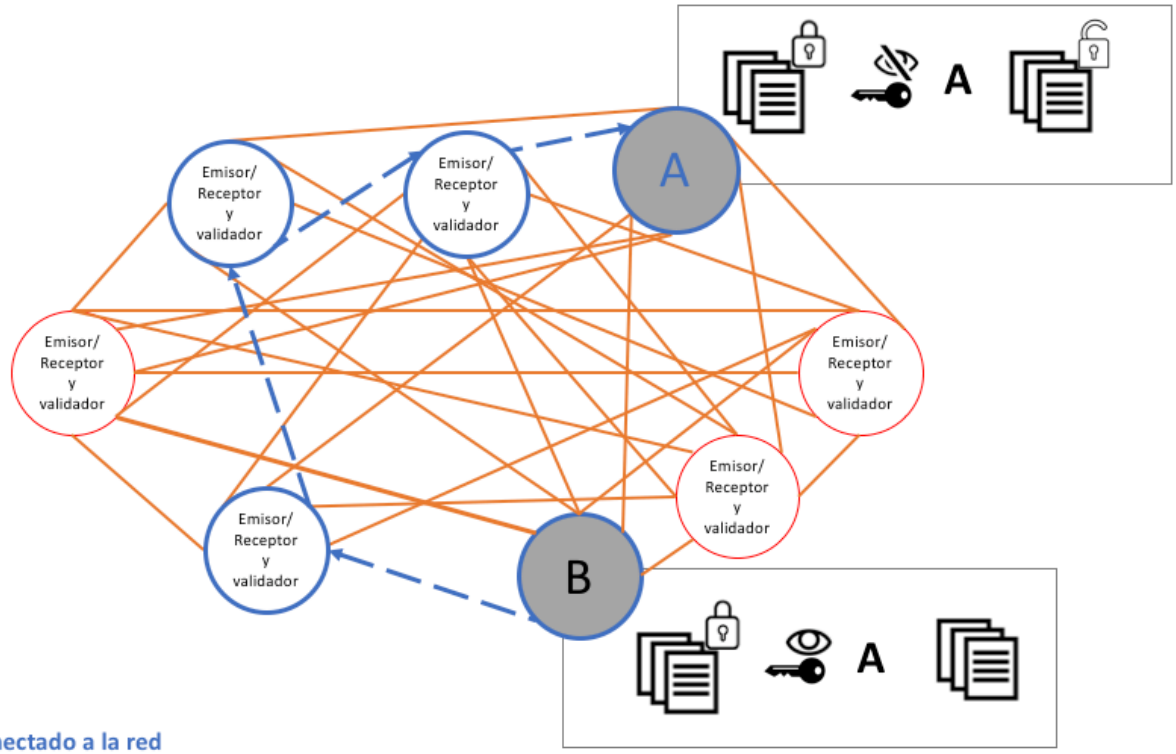


Fuente: elaboración propia

“La criptografía simétrica utiliza una sola clave tanto para cifrar un mensaje como para descifrarlo. En los primeros tiempos de esta disciplina, la seguridad de los mensajes cifrados se basaba en el uso de algoritmos secretos. El problema era que cualquiera que conociera su clave podía descifrarlos. En la actualidad los algoritmos más usados son de dominio público y conocidos por todos, por lo que la seguridad se basa en una clave y sólo aquellos que la conocen pueden descifrar el mensaje” (Núñez Miller: 207).

Para solucionar el problema que genera estos inconvenientes se ha creado el sistema de criptografía asimétrica, que es precisamente el que emplea *blockchain*. Mirar figura V.

FIGURA V: EMPLEO DE LA CRIPTOGRAFÍA ASIMÉTRICA PARA LA TRANSMISIÓN DE UN MENSAJE



Fuente: Elaboración propia

En este caso, B emplea la clave pública (y conocida) de A para cifrar el mensaje. Ese mensaje va por la red y todo el mundo lo puede ver, pero únicamente podrá ser descodificado por la persona que tenga la clave privada que corresponda a la clave

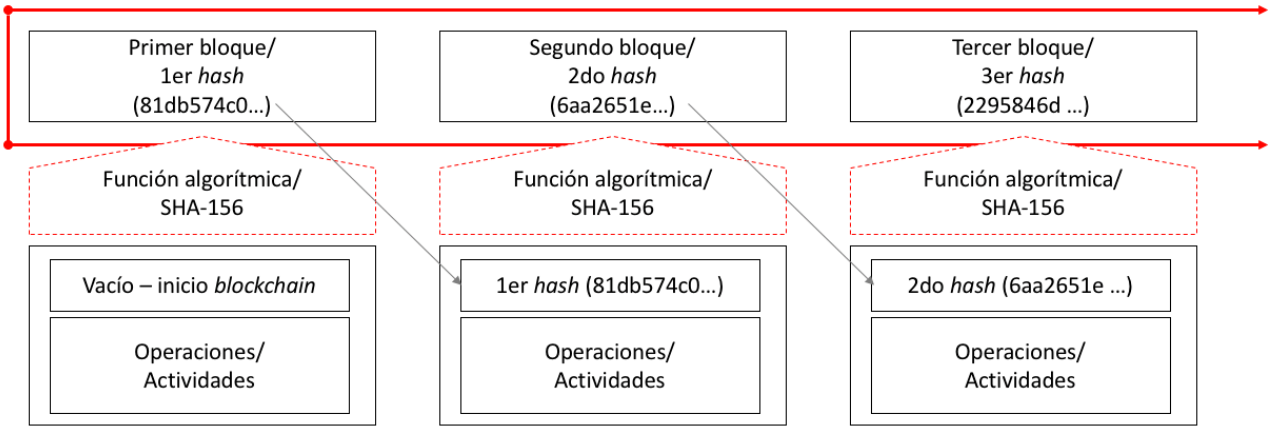
pública. De esta manera los usuarios no tienen porqué salir de la red para poder pasar la clave y están protegidos de ataques a terceros.

Funcionamiento de una cadena de bloques

El funcionamiento de una *blockchain* es el siguiente:

1. Se realizan una serie de operaciones/actividades en el transcurso del tiempo. Pasado un periodo (generalmente corto, aunque depende de cómo este configurada la *blockchain*) se procederá a asentar toda esta información en un bloque por medio de alguno de los métodos de prueba que se estudian a continuación.
2. Independientemente del método que se emplee, todas las actividades/operaciones mencionadas en el apartado anterior se condensarán en un *hash* (una combinación alfanumérica única de una cantidad fija de caracteres y que surge de aplicar el algoritmo *SHA-256* -*Security Hash Algorithm*- sobre un conjunto de información), que constituyen un bloque:
    a. En caso de ser el primer *hash* de la cadena, no habrá nada que añadir al comienzo de la operación/actividad.
    b. Para todos los *hashes* posteriores, el comienzo de la información que contenga tendrá que ser el *hash* anterior, dando lugar a un nuevo bloque único que dependerá del *hash* anterior y la información correspondiente; se ira construyendo una cadena en la que, al alterar cualquier bloque (contenido en *hashes*) provocará que todo lo posterior no corresponda con el hash previo, rompiendo la cadena. Véase figura VI.

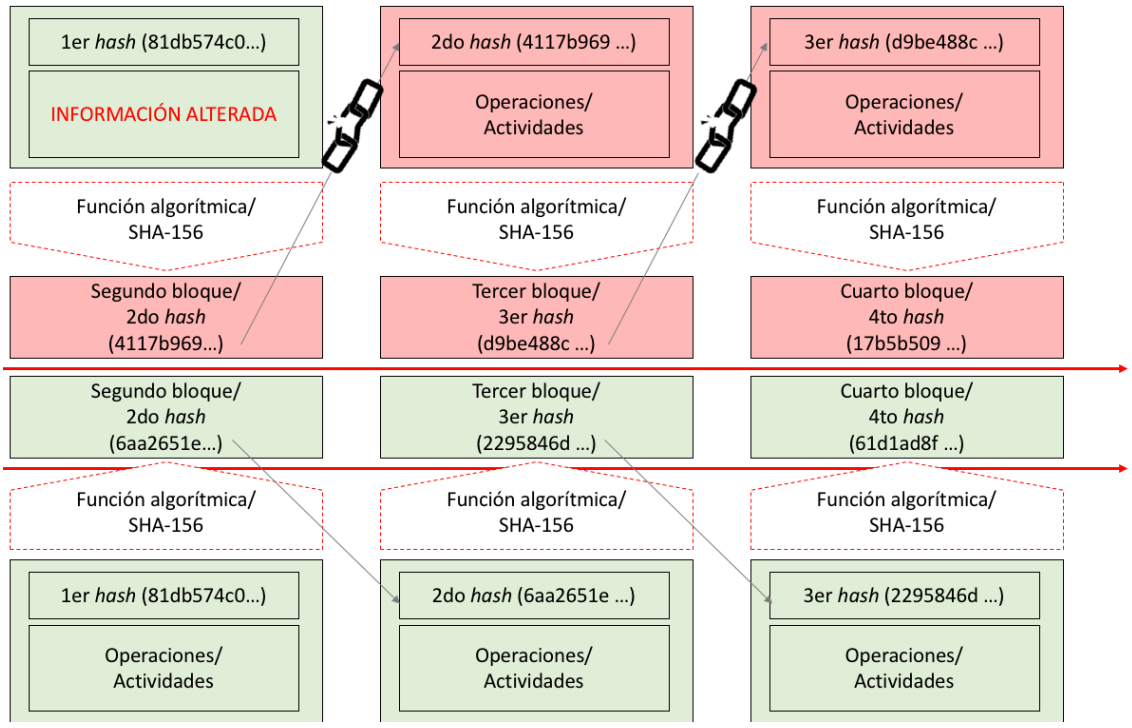
FIGURA VI: INICIO Y FUNCIONAMIENTO DE UNA CADENA DE BLOQUES



Fuente: elaboración propia

En otras palabras, todo bloque que no sea el de origen, tiene contenida la información de lo que ha pasado en el periodo de su creación y, además, al *hash* que forma el bloque anterior. Si se cambia cualquier bloque, este cambio (por mínimo que sea) alterará su *hash* y, por ende, el bloque siguiente del que forma parte, el cual variará y provocará a su vez una variación en el resto de la cadena. Véase figura VII.

FIGURA VII: RUPTURA DE UNA CADENA DE BLOQUES



Fuente: elaboración propia

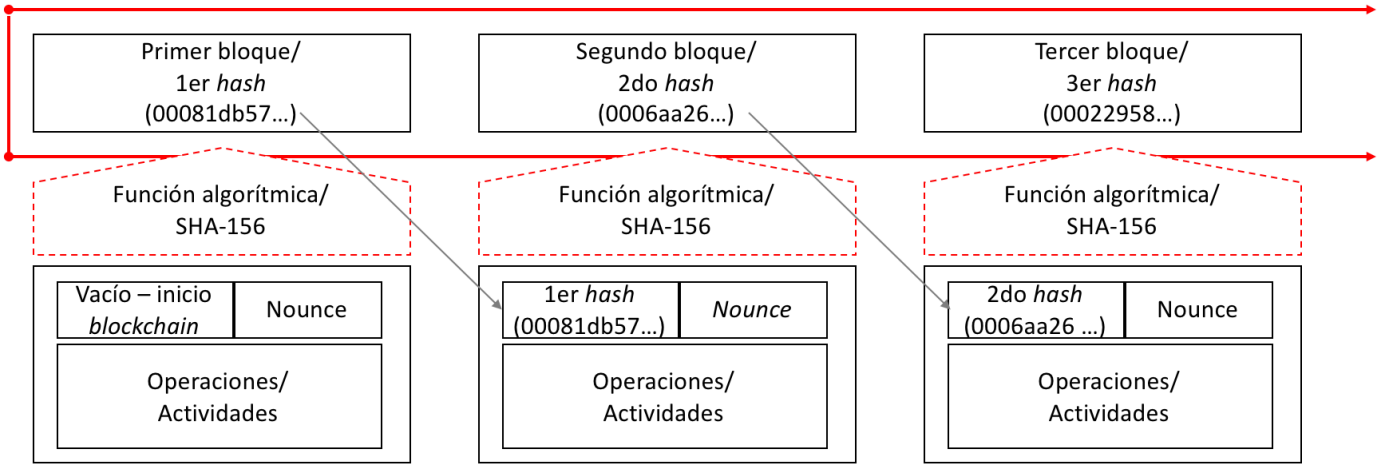
3. La cadena de bloques se va generando y, a medida que avanza, hace aún más difícil que se pueda realizar cualquier cambio.

Métodos de prueba

Hemos podido ver la relación que existe en la cadena, donde el cambio en una provoca la ruptura de la cadena entera. Esto convierte el sistema en algo totalmente fiable por sí mismo. Ahora bien, la formación de cada uno de los bloques necesita de un método de verificación. El método del trabajo (*proof of work*) y el método de la participación son los más extendidos.

Prueba de trabajo: Este es el método más conocido. Como indica su propio nombre, exige la realización de un trabajo concreto para la verificación de cada bloque. Este es el caso de *Bitcoin*, donde los *hashes* tienen que empezar con cuatro ceros. Para conseguir esto hay que añadir al bloque un *nounce* que permite que el *hash* resultante cumpla los requisitos. Véase figura VIII

FIGURA VIII: FUNCIONAMIENTO DEL MÉTODO PRUEBA DE TRABAJO EN LA *BLOCKCHAIN*



Fuente: elaboración propia

Aunque aquí el proceso está explicado de manera simple, la cantidad de trabajo y consumo de energía realizado son enormes, lo cual hace prácticamente imposible fundar grandes cadenas *blockchain* con este método: seguramente sea uno de los retos de la permanencia de *Bitcoin*, donde los mineros tienen "granjas de minería", que son

grandes polígonos donde hay procesadores consumiendo enormes cantidades de energía.

En *Bitcoin* el método de prueba de trabajo funciona así[4]: "*The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.*" (Nakamoto, 2008, 3)

Prueba de participación: Este caso es diferente. Uno de sus mayores promotores es *Vitalik Buterin*, que a pesar de utilizar en la primera versión de *Ethereum* el método de prueba de trabajo, se dio cuenta de que la cantidad de energía consumida para poder instalar un bloque en la cadena era enorme (Buterin, 2016). Por tanto, fundamenta un nuevo método de prueba en función de la participación que se tenga dentro de la *blockchain* (por ejemplo, en el caso de *Ethereum*, la cantidad de *ETHs* que tenga una persona). A medida que esta participación sea mayor, mayor será las opciones de ser el usuario que ratifique el bloque y buscará, supuestamente, el bien de la cadena y del bloque ya que, en caso contrario, estaría tirando una piedra contra su propio tejado (recordemos que el validador, que no minero, tiene una participación, en mayor o menor medida, por lo que no quiere que su participación se vea afectada por la conducta maliciosa de ningún usuario).

Buterin, (2017) explica como se implementaría el proof of stake en Ethereum: "*Proof of Stake (PoS) is a category of consensus algorithms for public blockchains that depend on a validator's economic stake in the network. In proof of work (PoW) based public blockchains (e.g. Bitcoin and the current implementation of Ethereum), the algorithm rewards participants who solve cryptographic puzzles in order to validate transactions and create new blocks (i.e. mining). In PoS-based public blockchains (e.g. Ethereum's upcoming Casper implementation), a set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its*

[4] Traducción: "La prueba de trabajo implica escanear el valor que, cuando *hasheado*, con el, por ejemplo, SHA-256, el *hash* resultante empiece con un número de cero *bits.* El trabajo medio necesario es exponencial al número de vero bits fijados y puede ser ratificado por ejecutar el propio *hash."* (traducción propia)

deposit (i.e. stake). Significant advantages of PoS include security, reduced risk of centralization, and energy efficiency.

In general, a proof of stake algorithm looks as follows. The blockchain keeps track of a set of validators, and anyone who holds the blockchain's base cryptocurrency (in Ethereum's case, ether) can become a validator by sending a special type of transaction that locks up their ether into a deposit. The process of creating and agreeing to new blocks is then done through a consensus algorithm that all current validators can participate in."[5] (Buterin, 2017)

Existen otros métodos de prueba que están en desarrollo o son meros planteamientos teóricos. Se hace una breve mención de los mismos: prueba mixta, de actividad, de capacidad, de almacenamiento y de destrucción.

Tipos de *blockchain*

Una cadena de bloques puede ser estructurada de tres maneras distintas: pública (*Bitcoin*), semiprivada (Alastria) o privada.

Pública: Este tipo de *blockchain* permite a cualquier usuario formar parte de la red y ser un nodo validador. Es el caso de *Bitcoin*, donde un usuario puede descargarse el código en cualquier momento y formar parte de la red. Todo lo que ocurre en la red es

[5] Traducción: "El método de prueba de participación (*PoS*) es una manera de consenso algorítmico para *blockchains* públicas que depende en la cantidad económica que el validador posea en la red. En el método de prueba del trabajo (*PoW*) en el que se fundamentan *blockchains* públicas (ejemplo: *Bitcoin* y la versión actual de *Ethereum*), el algoritmo recompensa a los que resuelvan un puzzle criptográfico que valide las transacciones y cree un nuevo bloque (ejemplo: minar). En el *PoS* de redes públicas (el caso de Casper, la nueva versión de *Ethereum*), un conjunto de validadores dispone de turnos proponiendo y votando el siguiente bloque, y el peso de cada voto depende del tamaño de su depósito (participación). Tiene importantes ventajas como seguridad, reduce el riesgo de centralización y eficiencia energética

En general, el método de prueba de participación funciona de la siguiente manera. La *blockchain* mantiene el conocimiento de un conjunto de validadores y cualquiera que tenga dinero de la *blockchain* (en el caso de *Ethereum, ether*) puede convertirse en validador haciendo un tipo de transacción especial que bloquea el *ether* en un depósito. El proceso de creación y acuerdo de los bloques es realizado por un algoritmo de consenso en el que todos los validadores pueden participar." (traducción propia)

visible para todos los usuarios (transmitiéndose la información encriptada, pero a la vista de todos).

Privada: Por ahora es el tipo de *blockchain* menos desarrollado. Puede tener grandes aplicaciones para contabilidad y demás procedimientos dentro de las empresas que no tienen por qué estar a la vista del público en general. En este caso los nodos validadores serían limitados y de acceso por invitación.

Semiprivada: Sería el caso de Alastria. La idea es que, a pesar de que los usuarios pueden ser anónimos, hay determinada información que se puede mantener privada, pero compartir en determinadas ocasiones con alguno de los usuarios, como cuando la Agencia Tributaria necesita hacer una investigación o cuando el banco quiera acceder a determinada información para decidir si conceder o no un préstamo. Además, los nodos validadores serán un conjunto de nodos, mientas que los demás no podrán validar, pero sí beneficiarse de las ventajas de la cadena.

En cualquier caso, hay que tener siempre en cuenta que, uno de los principios elementales de la *blockchain* – y el mundo de la programación en general – no se ve afectado por el tipo de cadena: compartir el código. Como ya se comenta en el proyecto, *Bitcoin* es una fuente abierta a todo el mundo que sirve para formar nuevas tecnologías a partir de la misma (*Ethereum* sobre *Bitcoin* o la propia Alastria sobre una versión de Ethereum). Los programadores pueden seguir teniendo acceso pleno a los códigos que permiten mejorar la tecnología mientras que la información dentro de cada *blockchain* se mantiene privada (si esa es la voluntad) o pública[6].

2.2.- ¿Un avance tecnológico o un avance intelectual?

La *blockchain* es la organización de unos conocimientos que ya se tenían desde hace tiempo. La pregunta en cuestión pretende averiguar si la *blockchain* podría haberse utilizado desde el comienzo del uso del internet o ha necesitado del nivel actual de tecnología para poder implementarse.

[6] https://github.com/alastria

La *blockchain* establece unas reglas del juego que lo hacen muy complicado de quebrar y, aún quebrado, es capaz de sanarse y no afectar al conjunto del sistema. La gran aportación del escrito de *Bitcoin* mencionado no fue la de construir un nuevo ordenador con un procesador único o la creación de una base de datos individual e inatacable; podría decirse que la gran aportación de la *blockchain* es precisamente la arquitectura de ese protocolo fiable que permite a la red adquirir mayor transparencia y disminuir los costes de intermediación.

Esta reflexión fue planteada ante diversas personas entrevistadas:

Por un lado, Daniel Díez García e Ignacio López del Moral, no respondieron a esta pregunta de una manera concreta. Hicieron un análisis en el que explicaron que más que una necesidad tecnológica, la *blockchain* es una nueva capa del internet, sobre la que se puede realizar todo lo que ya se hacía y que no existe una gran diferencia entre haberla desarrollado al comienzo de la era de internet o en el presente.

Por otro lado, en la entrevista realizada a José Luis Gahete Díaz, David Contreras Bárcena e Israel Alonso Martínez son de la opinión de que nos encontramos ante una idea que podría haber sido desarrollada hace más tiempo. Evidentemente, la tecnología ha mejorado, sobre todo en temas de criptografía y protección de la información.

2.3.- Estudio de las opciones de desarrollo práctico

Ahora bien, cabe plantearse hasta dónde se puede llevar esta nueva tecnología y su verdadero alcance. Autores como Tascopt D. y Tascopt A. (2017) dicen en su libro que lo que interesa es la tecnología detrás de *Bitcoin*, mientras que Preukschat A. en una charla impartida en ICADE en enero de 2018, afirma que la *blockchain* no puede ser entendida sin *Bitcoin*.

En principio, ambas posturas son conciliables. Es verdad que, sin el manuscrito de *Bitcoin*, la *blockchain* habría tardado aún un periodo superior en salir a la luz, pero también es cierto que el valor actual de las criptomonedas es puramente especulativo, y así lo refleja *Vitalik Buterin* a través de la red social twitter. Por tanto, hay que ver qué es lo que genera tanta ilusión entre los especuladores.

La duda es ¿Cómo se puede desarrollar la *blockchain*? ¿Qué recorrido tiene? Algunos llaman a la *blockchain* como "la revolución industrial del internet" -el propio título del libro de Alex Preukschat-, pero ¿Es tan fuerte su impulso? Como hemos concluido en el apartado anterior, el avance de la tecnología junto con la capacidad intelectual de determinados individuos, han llevado a la creación de la *blockchain*. Sin embargo, no es más que eso, un concepto, y por tanto tiene una amplia posibilidad de desarrollo.

Esto significa que el concepto nos da unas bases sobre las que funcionar; ejemplo de ellos es el siguiente paso dado por la red *Ethereum* sobre *Bitcoin*. La segunda, que es anterior en el tiempo, tiene un programa más sencillo donde la información que se queda es "Pedro da 2 *bitcoins* a Juan": un simple mandato; sin embargo, *Ethereum*, construida sobre la misma se fundamenta en el concepto de *Smart Contract*, de mayor complejidad: no es solo un información sobre una transacción económica, sino que crea un contrato autoejecutable en el que se pueden hasta llegar a dar condiciones simples para que se ejecute: "Juan paga 2 *ethers* a Pedro en el momento que este tenga más de 10 *ethers* en su cuenta". Para Ignacio López del Moral, este tipo de tecnología empleada en Ethereum puede tener una amplia implicación legal, simplificando una gran cantidad de contratos, creándose hipotecas autoejecutables o contratos de crédito de igual manera. Los *Smart Contracts* son seguramente un paso adelante en la tecnología *blockchain*.

El recorrido que tiene es aún superior: la tecnología puede acoger una mayor cantidad de problemáticas si, por ejemplo, hubiese una forma segura de meter información correcta en la *blockchain*. En una charla, el profesor don Javier Wenceslao Ibáñez considera que una fuente segura de información podría ser la de un notario, que tuviese la función de fedatario público dentro de la propia cadena de bloques.

Cabe decir aquí el carácter anarco-capitalista original de los creadores de la *blockchain*: la intención original era terminar con las estructuras centralizadas; ideas como una red semiprivada o el empleo del notario como fedatario público puede llegar a parecer que va contra los principios de los creadores o que se desvirtúa la idea original. En cualquier caso, a la hora de desarrollar nuevas cadenas de bloques, convendría emplear todos los medios disponibles para poder conseguir el objetivo propuesto de llevar la *blockchain* a otro nivel y llegar a buen puerto. Por ejemplo, se puede emplear

blockchain para contratos de crédito y de hipoteca; mientras que los primeros sí que pueden ser auto-ejecutados automáticamente, los segundos necesitan de un fedatario público que controle la información aportada. Lo propio sería combinar ambos puntos de vista para poder llevar la *blockchain* a su mayor potencial y desarrollo.

2.4.- Principales aplicaciones

Este punto ya va a tener una mayor orientación al objetivo del trabajo. Las aplicaciones sobre *blockchain* son infinitas (en todo lo que se puede utilizar la tecnología, se puede utilizar *blockchain*). Por tanto, en este apartado se va a analizar las facetas en las que ya está implementado o donde su aplicación es más clara y aquellos usos que podrían llegar a tener un mayor efecto sobre nuestro tema de ONGs.

Como primera gran función hay que acudir a lo que dice en *Bitcoin, a peer-to-peer electronic cash* system, Satoshi Nakamoto. La *blockchain* pretende resolver el problema del doble gasto: "*We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power*"[7] (Nakamoto ,2008, 8). Como principal aplicación de *blockchain* está la de resolver el doble gasto y crear activos únicos dentro de internet.

[7] "Hemos propuesto un sistema para transacciones electrónicas sin depender en confianza. Comenzamos con el marco habitual de monedas hechas de firmas digitales, el cual provee un control fuerte de propiedad, pero es incompleto sino existe una forma de prevenir doble-gasto. Para solucionar esto, hemos propuesto una red usuario-a-usuario que utiliza prueba-de-trabajo para registrar una historia pública de transacciones la cual rápidamente se convierte impráctica computacionalmente para que un atacante pueda cambiar si nodos honestos controlan la mayoría del poder de CPU" Traducido por Ángel León (https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf)

Finanzas

Sobre este punto, fue muy interesante la entrevista realizada con Daniel Díez García e Ignacio López del Moral. Estuvimos divagando sobre la necesidad, o no, de transformar todo en *blockchain* o solo ir haciendo mejoras donde haya margen para ello. Su opinión era la de mantener las cosas que ya se hacen bien y mejorar en los aspectos que se puedan. Un ejemplo muy sencillo de entender fue el que explicó John Whelan en el Banco Santander sobre el caso de las transferencias:

A nivel nacional tenemos herramientas que nos permiten hacer todo con celeridad y facilidad (como es el caso de *bizum*), mientras que a nivel internacional las dificultades son mayores: Se tiene que notificar al banco que recibe el dinero en el extranjero, el banco extranjero comprueba que existen los fondos… y se acaba dando un proceso de varios días e incluso semanas. En este caso, la aplicación de la *blockchain* en transferencias nacionales no tiene mucho sentido (*bizum* es una plataforma que funciona perfectamente en cuestión de segundos), sin embargo, en transferencias internacionales, *blockchain* puede ser una de las mejores alternativas para convertirlo en un sistema más eficiente.

Por tanto, en el mundo estricto de las finanzas (y dejando al margen elementos de seguimiento o transparencia, de los que se habla posteriormente), la *blockchain* puede provocar grandes avances en situaciones donde no se había conseguido realizar ningún cambio (el caso de las transferencias internacionales mencionado arriba), sin embargo, no parece tan útil para otras funciones que ya funcionan con una gran facilidad y agilidad.

Gobierno

En el capítulo "participación ciudadana y voto" de la obra "*Blockchain*, la revolución industrial del internet" (Lage Serrano, 2017, 101) pone en relieve los cuatro principales problemas que tiene el voto online y la participación en los proyectos de gobierno:

1. Es necesario una autenticación fuerte para identificar la identidad del votante
2. El anonimato, para que nadie que tenga acceso a los votos pueda identificar quien lo ha realizado
3. Auditibilidad, del proceso y la plataforma

4. Inalterabilidad del voto

3.- ONGs y sus proyectos

3.1.- ¿Qué es una ONG?

Como podemos ver, una ONG tiene varias y diversas acepciones, desde unas más técnicas a otras más funcionales. De hecho, (Ruíz Olabuenaga, 2000, 32) muestra la difícil determinación del término ONG en España: "El estudio del sector no lucrativo o tercer sector español adolece, como se ve, de una doble imprevisión terminológica. Por un lado, no se dispone de un concepto preciso y comprehensivo y, por otro, el sector tiende a identificarse con conceptos parciales tales como el de economía social, el de sociedad civil, el del conjunto de organizaciones voluntarias o del de las no gubernamentales. La simple enumeración de términos tan heterogéneos permite concluir lo que, en término generales, es un sentir común, como afirman Santiago Álvarez y otros, que 'la aventura de arriesgar una definición parece estar condenada desde el principio al fracaso más absoluto… Si bien nadie duda de la existencia y peso de este sector, es preciso observar que se ha prestado poca atención al problema básico de cómo se define el sector qué realidades contiene"

Sin embargo, esa aventura de la que nos habla Santiago Álvarez es emprendida por algunos como el comité español de ACNUR, para los cuales la definición de una ONG es como sigue: "Las ONG son organizaciones independientes y sin ánimo de lucro que surgen a raíz de iniciativas civiles y populares y que por lo general están vinculadas a proyectos sociales, culturales, de desarrollo u otros que generen cambios estructurales en determinados espacios, comunidades, regiones o países.

Hoy día es casi común hablar de ellas cuando se abordan valores como la cooperación, la solidaridad, la ayuda desinteresada y el altruismo. También solemos asociarlas a las labores de voluntariado en cualquier sector o área de intervención." (ACNUR)

Otros, como es el caso de García Izquierdo (1999) hacen una respuesta más técnica: "Término acuñado pen el ECOSOC (Consejo Económico y Social de la Organización de las Naciones Unidas) en el momento de configuración de los diferentes organismos de

Naciones Unidas, para distinguirlas de las entidades de las representaciones oficiales" (García Izquierdo, 1999, 557)

En cualquiera de los casos, para la realización de este proyecto se entiende por ONG la concepción más amplia posible, ya que en realidad lo que se plantea es la aplicación de la *blockchain* en cualquiera de actividades realizadas por el tercer sector. Se entienden por sinónimos términos que pueden ser distintos: tercer sector, ONG, organizaciones sin ánimo de lucro, sociedades civiles…, aunque sí se guardará cierta diferenciación con la economía social (explicado más adelante). Por tanto, a la hora de definir que es una ONG, se está de acuerdo palabras de Jiménez Lara (2003): "El sector no lucrativo en su conjunto, como respuesta que es a la dinámica profunda de la sociedad, experimenta, al igual que ella, un influjo pluridimensional que se manifiesta en una diversificación progresiva de las instituciones que lo componen." (Jiménez Lara, 2006, 27)

3.2.- Principales características

Si bien hemos podido ver cómo el concepto de ONG o sector sociales es amplio y no cerrado, Salas (2009) saca una serie de características de toda actividad o proyecto del tercer sector:

1. Tienen que estructurarse internamente. Deben guardar un orden propio que les permita realizar sus actividades. No se entiende, por tanto, como sector social una actividad altruista sin ningún tipo de organización como podría ser los alumnos de un colegio yendo a visitar ancianos a no ser que este organizado por otra entidad que se dedique a ello. Tiene, por tanto, "una estructura interna, con estabilidad relativa de actividades y objetivos." (Salas, 2009, 30)
2. Entidades privadas. Ello implica que no pueden ser dependientes del Estado ni de la administración pública, tanto en la faceta jurídica como en la estructural. Esto no es impedimento para recibir financiación pública.
3. Sin ánimo de lucro. Esto no implica que la organización no obtenga beneficios, significa que la aportación realizada por los fundadores, socios o creadores tiene que ser de manera onerosa, sin esperar nada a cambio y que, por tanto, los

beneficios se reinviertan en continuar implementando el fin social al que se dedica la entidad.

4. Con capacidad de autogobierno. Relacionado con el primer punto, dentro de la estructura organizativa, tiene que haber unos estatutos o pautas que establezcan como se va a gobernar la entidad.
5. Participación voluntaria, siendo los voluntarios la mano de obra y fuente del trabajo realizado por la entidad

Sobre estos elementos se pueden dar algunas características de la economía social, pero es importante saber que se trata de elementos diferenciados. Los principales elementos de la economía social son:

1. "Primacía de las personas y del objeto social sobre el capital.
2. Adhesión voluntaria y abierta y control democrático por sus miembros desde la base
3. Conjunción de los intereses de los miembros, usuarios y/o interés general
4. Defensa y aplicación del principio de solidaridad y de responsabilidad
5. Autonomía de gestión e independencia de los poderes públicos
6. Aplicación de los excedentes al objeto social mediante la reinversión o distribución según los deseos de sus miembros para la creación de empleo, de actividades de nuevas empresas, retorno de capitales invertidos y servicio a los miembros, entre otros" (Salas, 2009, 32)

3.3.- Principales funciones

En la entrevista realizada a Manuel Hurtado, dijo que uno de los grandes retos ante los que una ONG se encuentra es la de aportar valor: para él todas las nuevas tecnologías, no solo la *blockchain,* están creando un mercado de cada vez mayor eficiencia donde había cosas que antes eran relativamente inviables, pero ahora son simples de hacer, dando una mayor flexibilidad a las actividades (como sería el caso de las microdonaciones). Por tanto, esta nueva ola tecnológica, de la que ve a la *blockchain* como uno de los principales impulsores en el tercer sector, va a provocar que solo permanezcan vivas las ONGs que verdaderamente aportan un valor (ya sea porque su actividad es única, como podría ser un voluntariado con la gente más desfavorecida de

un país del tercer mundo o, por otro lado, una entidad cuya forma de trabajar y estructura sea tan eficiente que le permita aportar valor a la sociedad al menor coste posible).

Añadido a esta opinión, conocidas las entidades, prácticas y características del tercer sector, en el presente punto se aborda lo que para Cabra de Luna (1998) son las principales funciones de una entidad del tercer sector:

Agente innovador. Las ONGs tienen la necesidad de ser innovadoras; se encuentran en un mundo de constante cambio donde las eficiencias hacen reducir los costes de manera exponencial. Como hemos visto, es necesario que tengan cierta organización interna y unos beneficios que les permitan mantenerse para poder cumplir con su función y objeto sociales. Es precisamente esta faceta de estar a la vanguardia en las nuevas tecnologías e ideas lo que les permite cumplir con los objetivos y, de la mano del trabajo de los voluntarios, convertirlo en entidades que pueden prestar y producir servicios (de los que se habla a continuación) a la sociedad.

Agente productor y prestador de servicios: Como bien mantenía Manuel Hurtado, es necesario que la ONG aporte valor, el que se materializa a través de un bien o servicio. Las entidades del tercer sector y sus proyectos están destinados a satisfacer necesidades que no son satisfechas en el libre mercado, bien porque no sea rentable, bien sea porque no son producidas. Los servicios y bienes aportados por la entidad son su valor añadido, pero para poder mantenerse, debido al reducido volumen de ingresos, necesitan abaratar lo mayor posible en costes, es decir, ser lo más eficientes posible.

Agente mediador: Las entidades del tercer sector ponen en contacto dos mundos: por un lado, las personas que tienen recursos y quieren ayudar (ya sea económicamente o con su trabajo) y, por otro, el grupo social que tiene necesidades. Añadido al argumento de aportar valor, esta es otra de las funciones clave. Cuanto mejor mediadora sea una entidad, mayor será su valor aportado a la sociedad receptora y, por tanto, mejor cumplirá su objeto social.

Agente defensor: Mantiene una alta relación con el punto anterior. Como se puede apreciar en el apartado “un registro público basado en la *blockchain*”, una de las funciones principales de un proyecto social es la de actuar como defensor de la parte

ayudada respecto de las posibles desventajas que pueda estar sufriendo. Esta defensa supone, en sí misma, una aportación de valor. En palabras de Salas (2009) una ONG es agente defensor "cuando se encarga de velar por los intereses y derechos de determinados grupos, o bien actúan como agente reformador, cuando intervienen de forma conjunta para presionar e influir en la opinión pública y la política, buscando cambios legislativos." (Salas, 2009, 33).

Agente preservador de valores sociales: Su presencia hace que se mantenga la conciencia social activa (un ejemplo claro sería las grandes catástrofes o desigualdades y la rápida intervención de las ONGs). "Es inherente a la naturaleza, la estructura, la orientación y actividades que desarrollan las entidades a favor de una sociedad mucho más solidaria y tolerante, convirtiéndose en el soporte mediante el cual se desarrollan acciones para que prospere la cultura del voluntariado, la participación, el altruismo, la solidaridad, la diversidad, el pluralismo, la multiculturalidad, el respeto mutuo, etc., reforzando así el sistema democrático y consolidando el tejido socia de un país." (Salas, 2009, 33).

Por tanto, la ONG tiene que encargase de aportar valor allí donde se encuentre. Para ello, cumple cinco funciones: innovar, aportar y crear servicios, mediar, defender y conservar los valores sociales.

4.- Aplicación de la tecnología en proyectos de ONGs

En el presente apartado se busca identificar, tras la revisión de la literatura y las entrevistas, cuáles son los principales retos a los que se enfrenta una actividad del tercer sector y posteriormente ver cuáles pueden ser solucionados por la *blockchain*.

4.1.- Problemática

Transparencia

Este es sin duda, para Moro (2009), el gran reto al que se tienen que enfrentar las ONGs y para ello hay que exponer, por las personas involucradas, la realidad en la que se encuentran.

Tras el escándalo de Interfom Oxfam publicado por *The Times* (O'neill, 2018), son muchas las grandes ONGs que han manifestado su intención de luchar desde dentro por esta transparencia: Catherin Illberg, asesora especial del Consejo Noruego para los Refugiados afirma: "Sabemos que la falta de información sobre este tipo de casos es común en la industria en su conjunto -y eso es probablemente lo que ha pasado-, pero estamos trabajando para aumentar el conocimiento sobre los mismos", Sam Smith, portavoz del Comité Internacional de la Cruz Roja dice: "Creemos que no se trata de una sola organización, sino que es un problema de todo el sector y debemos trabajar colectivamente para superarlo" (El economista, 14/2/2018)

Vernis (2004) considera de vital importancia la transparencia: "A menos que las organizaciones no lucrativas de nuestro país faciliten a la sociedad de una forma rigurosa información verídica y transparente de sus actuaciones, la confianza que la sociedad española sigue depositando en ellas se irá deteriorando" (Vernis, 2004, 174)

El principal y más complicado reto de una ONG es conseguir la transparencia de sus actividades. Ello implica, no únicamente una transparencia financiera (clásica concepción), si no que va un paso más allá: "No se trata simplemente de informar a la sociedad sobre los aspectos financieros de la entidad no lucrativa, sino que la tendencia actual es la de publicitar todos los procesos de gestión de la ONG. La relación entre rendir cuentas y la gestión es cada vez más palpable. Sin duda, la necesidad de realizar un mapa de los procesos más relevantes de la organización para mejorar el trabajo de la misma según las normas de calidad linda con la importancia de hacer visibles los procesos de gestión de la ONG. Cómo utiliza los recursos económicos, que proyectos lleva a cabo, cómo evalúa tales proyectos, si logran realizar los fines propuestos en la misión de la organización, cuál es el impacto social de tales proyectos, si sirven para incrementar la calidad de vida del colectivo beneficiario de la ONG, entre otras, son las preguntas a la que la organización debe dar respuesta y comunicar a los grupos de interés" (Moro, 2009, 146)

Sin duda, la confianza en las ONGs es uno de los principales problemas, hasta el punto de que, en 2016, el 56% de los españoles no realizó ninguna donación por dicho motivo (Asociación Española de Fundraising, 2016)

Aportar valor

Uno de los principales retos de las ONGs es el de aportar valor y no convertirse en meros intermediarios (aunque, como hemos visto, esto también puede ser fuente de valor y es una de las funciones principales de una ONG).

Mejorar las condiciones laborales.

"Las ONG saben que tienen a su favor que su personal tiene una alta motivación, incluso le han encontrado una denominación a la satisfacción que genera trabajar en el sector social entendiéndola como una parte de la contraprestación laboral: la famosa remuneración psicológica. Por ello, se amparan en este beneficio 'extra' para justificar una paga inferior a los parámetros normales, en un mercado laboral, como el español, en el que de por sí lo salario ya está por debajo de la media europea. No obstante, la alta motivación hay que mantenerla para seguir brindando un servicio de calidad y para ello hay que considerar al trabajador en sus expectativas y necesidades que varían a lo largo de su vida […] Si la organización no considera estas cuestiones básicas en su área de dirección de personas, va a perder no sólo el valor añadido de la alta motivación, sino que muy probablemente a la trabajadora también." (Moro, 2009, 539-540)

Se encuentran ante un reto muy importante en el que establecer un salario justo a los trabajadores que formen parte de la entidad, impulsando su productividad y monitorizando su producción sea un papel clave.

Plan estratégico

Los planes estratégicos son uno de los quebraderos de cabeza más fuertes que tienen las ONGs y los motivos de su posible fracaso, para Navajo (2009):

1. Una alta dirección que no apoya el plan y que además mantiene para su fuero interno los asuntos de mayor relevancia. Además, ello implica que no se suela tener en cuenta a toda la organización, pudiendo llegar a afectar en otros retos como la motivación laboral de la que ya se ha hablado.
2. Una planificación que se olvida del largo plazo, solucionando problemas a destiempo y rápidamente. Cubrir el corto plazo acaba provocando que las personas no tengan debidamente asumidas o interiorizadas sus

responsabilidades, no queden unos objetivos claros y no haya una visión sobre hacia dónde ir.

3. El plan busca solo la previsión, sin la intención de crear verdaderas conductas que permitan un desarrollo plano y continuo en los distintos objetivos fijados. Estas pautas generales provocan que, a la hora de la supervisión, no se sepa cuáles son los valores a evaluar o medir.
4. Confusión de lo que es un plan estratégico con un estudio
5. Y otros motivos como la creación de un plan estratégico por cumplir simplemente con la imagen, fijar una ruta inflexible (que derive en resistencia al cambio) o acomodar a la directiva.

4.2.- Solución con la aplicación de la tecnología

Hemos analizado los principales retos a los que se enfrentan las ONGs. Ahora bien, solo unos pueden ser resueltos por la tecnología *blockchain*, ya que no se trata de una solución a todos los problemas, sino de una herramienta que permite mejorar su actual funcionamiento. Por tanto, desde este trabajo se pretende tratar los tres principales retos en los que la *blockchain* pueden ayudar: transparencia, generación de valor y calidad de trabajo

Transparencia.

Respecto al primer problema mencionado, la transparencia, podemos afirmar sin duda que la tecnología *blockchain* es una herramienta con un gran potencial para solucionarlo o, como mínimo, mejorarlo. Así, vemos como nos encontramos ante una tecnología que contiene una información inmutable, lo que permite que, ante un cambio, salten las alarmas de todo el sistema y la cadena estaría rota desde el momento de la infracción. Además, al margen de esta inmutabilidad, una *blockchain* bien ordenada y con los correctos nodos que cumplan sus funciones podría llegar a tener un control apropiado sobre las tareas realizadas en la realidad. En otras palabras, aparte de exponer al público lo que ocurre, ¿De qué sirve que la actividad sea inmutable si una persona actúa como no debería, el daño ya estaría hecho, tanto para la sociedad como para la imagen de la entidad? La respuesta a esta pregunta se puede resumir en dos factores:

1. Por un lado, porque permitiría que se diese cuenta antes de tiempo de la situación ante la que se encuentran y activa unos mecanismos de pronta reacción.
2. Por otro, una correcta distribución de los nodos que forman parte del sistema, especialmente de los que están sobre el terreno (los trabajadores de la entidad), haría que se pudiese controlar el correcto funcionamiento; un buen ejemplo es el caso de iwillbe.org. Además, a este control entre los propios nodos de la información adoptada, se puede añadir el de las nuevas tecnologías.

Manuel Hurtado (2018a) describe como se implementa la transparencia en el caso de itwillbe.org: "A través de la plataforma creada […], los responsables de la donación pueden seguir los hitos del proyecto y ver en todo momento y en tiempo real qué dinero se ha gastado ya y en qué actividades" (Hurtado, 2018a).

Continúa explicando que se puede crear una serie de nodos que sean de control, incluido los propios receptores de la ayuda. Así, si un trabajador de la ONG se compromete a proveer a todos los jóvenes de los bienes básicos, se puede solicitar al vendedor de la tienda que se convierta en un nodo validador de la actividad del voluntario. Otro ejemplo sería: una de las personas que ha sido ayudada de joven, quiere seguir recibiendo el apoyo a medida que crece, este tiene que comprometerse a dar clase a los más pequeños todos los miércoles 2 horas. Para comprobarlo, se podría acceder a su geolocalización móvil, que quedaría registrada en la *blockchain* para gestionar toda la información.

En cualquier caso, a todo esto hay que añadirle la transparencia financiera absoluta, donde los donantes podrán ver que se hace con su dinero en todo momento. *Blockchain* abre las puertas, también, a las microdonaciones.

Se puede ver cómo la cadena de bloques es una solución real y lista para implementar ante uno de los principales problemas de las entidades del tercer sector.

Aportar valor

Es muy acuñado, últimamente, el término del internet del valor. Esta denominación se hace en contraste con la que se empleaba anteriormente del internet de la

información. En el segundo, la función principal del internet era transmitir información de un lado a otro, de un periodista a un mayor número de lectores. Era posible que una persona dijese a otra que estaba haciendo un fin de semana gracias a las redes sociales; el internet no es más que un mero altavoz de las cosas que se realizan.

Sin embargo, con el avance las tecnologías, ya no hablamos únicamente de un internet de la información. Hoy podemos transmitir, con mediana facilidad, cantidades de dinero a través de internet, hacer pagos con el móvil…

Y, uno de los grandes motivos de este cambio es la eliminación del doble gasto: da igual que un artículo de Facebook se publique y republique, a no ser que sea publicidad, ese documento o foto no genera ningún valor (tema distinto sería la confidencialidad del mencionado artículo); pero sí que sería un problema que los dos euros que le he enviado a mi hermano por *bizum* pudiese copiarlos y pegarlos cuantas veces quisiera. El internet del valor garantiza que los activos transmitidos de manera casi instantánea sean únicos y, por tanto, contengan valor en sí mismos.

Como hemos visto al principio del trabajo, la tecnología *blockchain* soluciona precisamente el problema del doble gasto y permite crear activos verdaderamente únicos. Hace que lo que este registrado en la propia cadena de bloques sea único y se pueda realizar transferencias a través de la misma.

Mejorar las condiciones laborales

A pesar de que las principales aplicaciones las podemos ver en los elementos anteriores, se puede crear a través de la *blockchain* un sistema democrático de pago para los trabajadores de la ONG, valorando su esfuerzo no solo con la mencionada "remuneración psicológica" de Moro (2009), si no también ajustando sus actividades (perfectamente definidas y guardadas) por medio de la *blockchain*.

De esta manera se podrán dar un salario más ajustado a las necesidades y trabajo del a persona.

5.- Aplicación práctica

En este apartado queremos dar una solución a diversos casos en los que se podría aplicar la tecnología *blockchain*. Como hemos podido ver, esta sirve para solucionar algunos de los problemas a los que se enfrentan los proyectos de ONGs, especialmente las de un tamaño reducido que tiene más dificultades para desarrollar sus actividades y que necesitan un especial apalancamiento en las nuevas tecnologías para alcanzar ese umbral de supervivencia.

Para ello, se van a crear casos o hipótesis producto de las conversaciones con las personas entrevistadas y lo aprendido durante el proyecto, junto con la experiencia personal.

5.1.- Aldeas infantiles

"Atendemos a niños y jóvenes que se encuentran en situación de vulnerabilidad, impulsando su desarrollo y autonomía, mediante el acogimiento en entornos familiares protectores y el fortalecimiento de sus redes familiares, sociales y comunitarias." (Aldeas Infantiles SOS)

La idea Aldeas Infantiles pretende dar una protección a niños que se quedan sin el cuidado de sus familias, en ambientes calmados y formadores; sus casas están distribuidas, en el caso de España, por todo el territorio nacional, en zonas apartadas de las grandes poblaciones y el régimen de visitas está limitado a los voluntarios que trabajan para la misma para poder mantener la tranquilidad ya mencionada.

Como podemos ver, Aldeas Infantiles tiene un gran plan entre manos y, consecuencia de su propia actividad, necesita cierta privacidad para que los jóvenes puedan crecer y madurar en un ambiente estable, donde hay personas comprometidas trabajando permanentemente y un grupo de voluntarios relativamente estable. Esto hace que se tenga que tener un especial cuidado con su transparencia funcional y financiera.

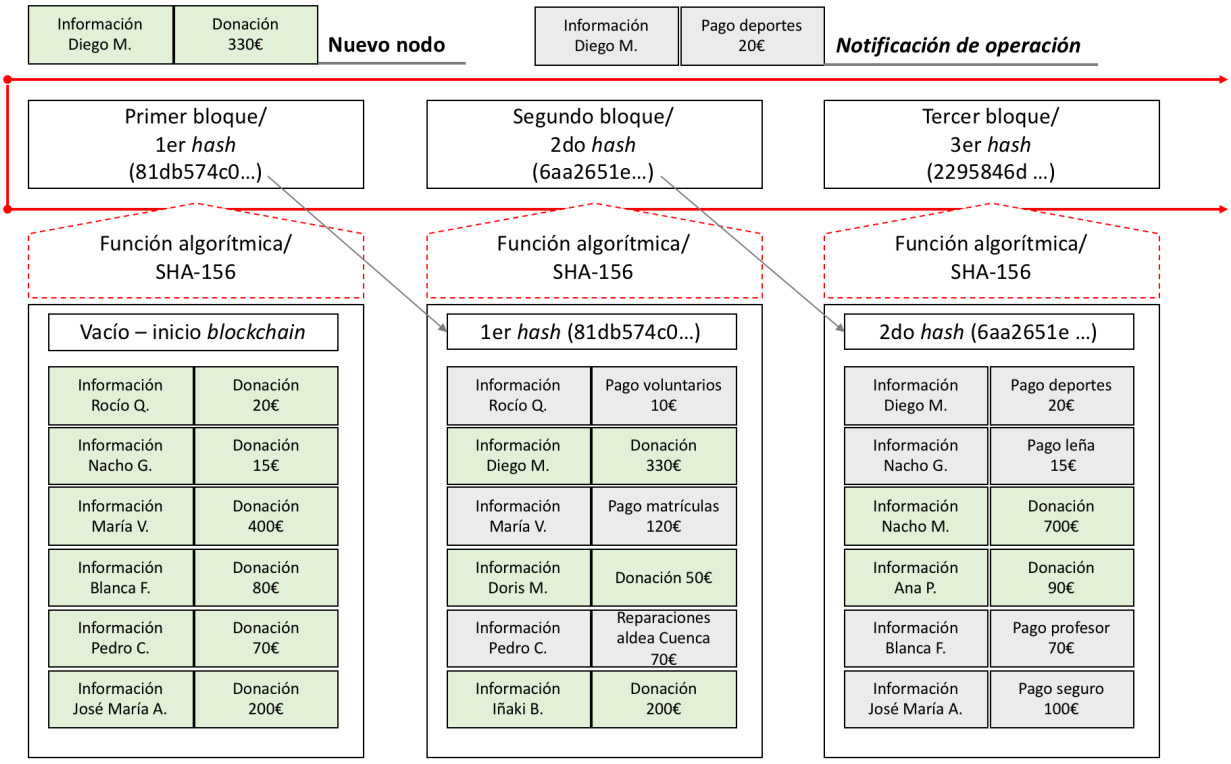
Hace ya tres meses realicé una donación en la calle a la ONG por medio de un voluntario de una manera poco segura, poniendo los datos de mi tarjeta de crédito en un papel oficial (del cual me dieron una copia) para hacer la donación. Aunque al principio no pensé los riesgos que tenía hacer la donación de esta manera, más tarde

me di cuenta del error que pude haber cometido. Confié en el buen hacer del voluntario y la entidad y, al tiempo (un mes), me llegó un mail de confirmación de la transferencia de parte de Aldeas Infantiles. De ahí en adelante no he recibido más noticias. Además, al preguntar al voluntario sobre la oportunidad de ir a ver alguna de las aldeas, me contó que solo algunos días se podía ir de visita a las mismas.

Por la experiencia vivida, se puede ver como Aldeas Infantiles puede mejorar, por un lado, su transparencia financiera y, por otro, la funcional.

La aplicación de la *blockchain* abre una gran gama de posibilidades. Para explicarlo, ciñámonos al ejemplo de mi donación desde una cuenta de crédito o por una tarjeta, se puede realizar el pago a través una plataforma *blockchain* privada o semipública que cree un nodo con la información de donante y que le permita "rastrear" los movimientos realizados con su dinero; es más, las donaciones en efectivo también podrían llevar este proceder si se identifica la cantidad aportada por cada donante y se registra sus datos en la plataforma (aunque sería, evidentemente, más costoso de esta manera). Así, cada una de las donaciones realizadas se introducen en la plataforma *blockchain* y cuando se hagan transacciones o transferencias con el dinero de uno de los donantes, este podrá ser informado (cierto es que sería informado en conceptos generales: "pago de la nómina" y no de asuntos concretos "pago de la nómina de Ignacio G."). En la figura VIII se puede ver cómo se programaría la *blockchain.*

FIGURA IX: PROGRAMACIÓN *BLOCKCHAIN* ALDEAS INFANTILES SOS



Fuente: Elaboración propia

Con esta nueva forma de tratarlo, al margen de determinar el método de prueba (que podría incluso llegar a no utilizarse ninguno ya que solo hay un nodo que participe activamente -Aldeas Infantiles-, y por tanto la *blockchain* se emplee como una red privada pura de información y control) se conseguiría mantener informado al donante, que puede recibir una notificación cuando se realicen operaciones con su dinero; en esta notificación habría que poner cuáles son los datos específicos (persona que realiza el gasto, cantidad empleada, lugar en el que se hace…). Además, la *blockchain* estaría programada para que cada usuario donante nuevo se convirtiese en un nodo propio, provocando varías cosas:

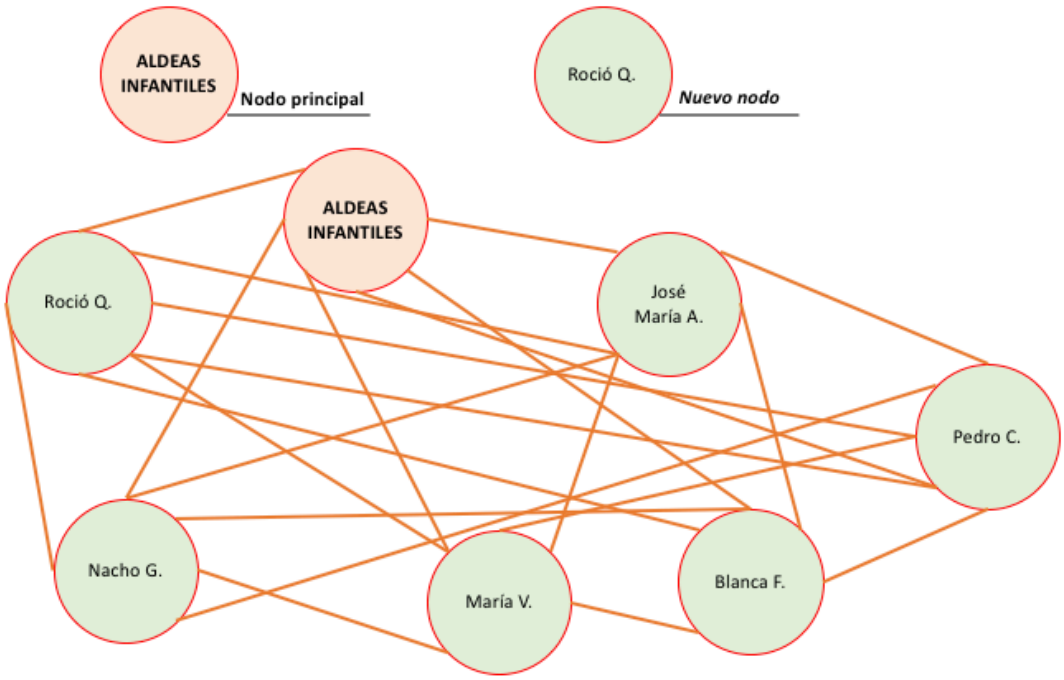
A medida que hubiese más donantes, de mayor seguridad será la red, ya que hay más usuarios y eso hace que sea más complicado una posible intrusión.

En segundo lugar, esto permitiría tener un mayor control sobre las actividades y el propio donante sabría en todo momento donde se está utilizando su dinero.

Además, cuando el dinero aportado por cada donante sea consumido, este estará al tanto y, en caso de estar contento con el trabajo realizado, podría realizar otra donación

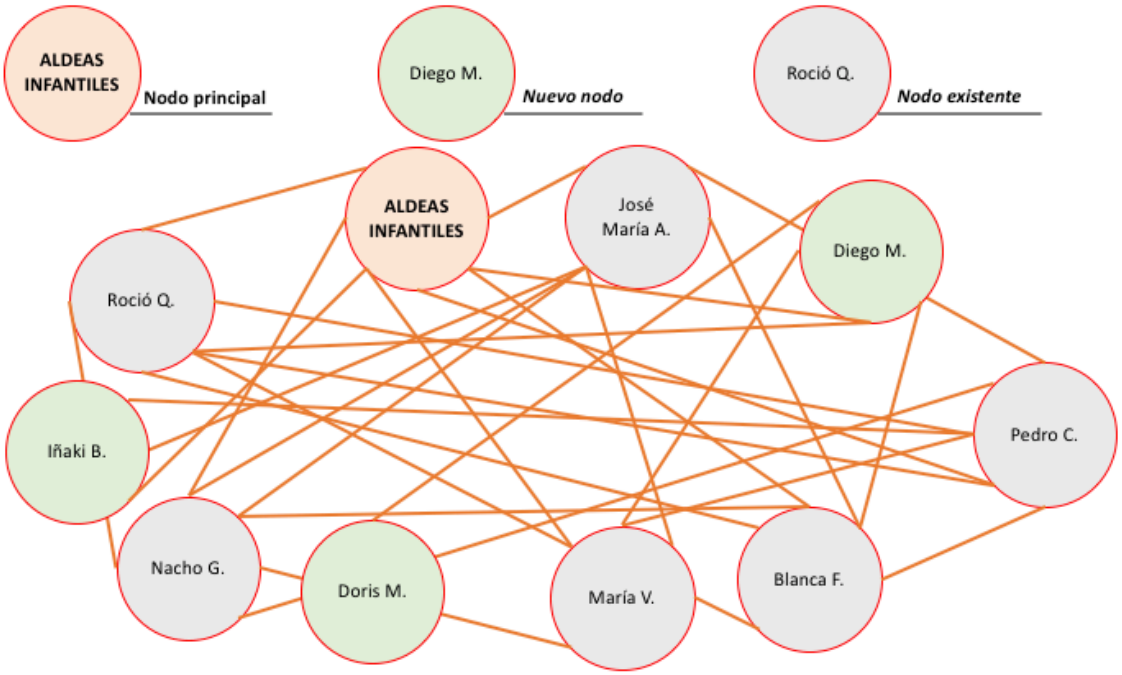
de una manera más rápida y eficaz, pudiendo llegar a mantener cierta fidelidad de donación y mejorando, por tanto, los ingresos de las ONGs.

FIGURA X: ESTRUCTURA DE LA RED DISTRIBUIDA ALDEAS INFANTILES SOS (I)



Fuente: Elaboración propia

FIGURA XI: ESTRUCTURA DE LA RED DISTRIBUIDA ALDEAS INFANTILES SOS (II)



Fuente: Elaboración propia

Como se puede ver en los gráficos IX (que corresponde con el primer bloque) y X (que corresponde con el segundo bloque) la red se iría formando en función de las donaciones realizadas. Al principio todos son nodos nuevos, pero a medida que pasa el tiempo y aumentan las donaciones, la red va ganando sostenibilidad y se pasa el número crítico de usuarios necesarios.

Por tanto, con la *blockchain* se abren muchas vías para el donante: en primer lugar, es más rápido, seguro y eficaz para la recolección de los pagos (aunque se hagan por medio de transferencia bancaría, se puede vincular dichas transacciones la cadena de bloques privada) permite agilizar un proceso largo y de escasa seguridad que podría echar atrás a potenciales donantes. Por otro lado, de manera automática se iría haciendo un registro de los distintos pagos realizados, los cuáles se podrían ir transmitiendo a los donantes y, lo que es más importante, cuando se haya consumido la donación, el mismo lo sabría y podría continuar involucrado en el proyecto.

Cabe mencionar también que emplear la *blockchain* facilita la realización de las microdonaciones, dando lugar a una nueva fuente de financiación que se está empezando a explotar por las ONGs con las nuevas tecnologías.

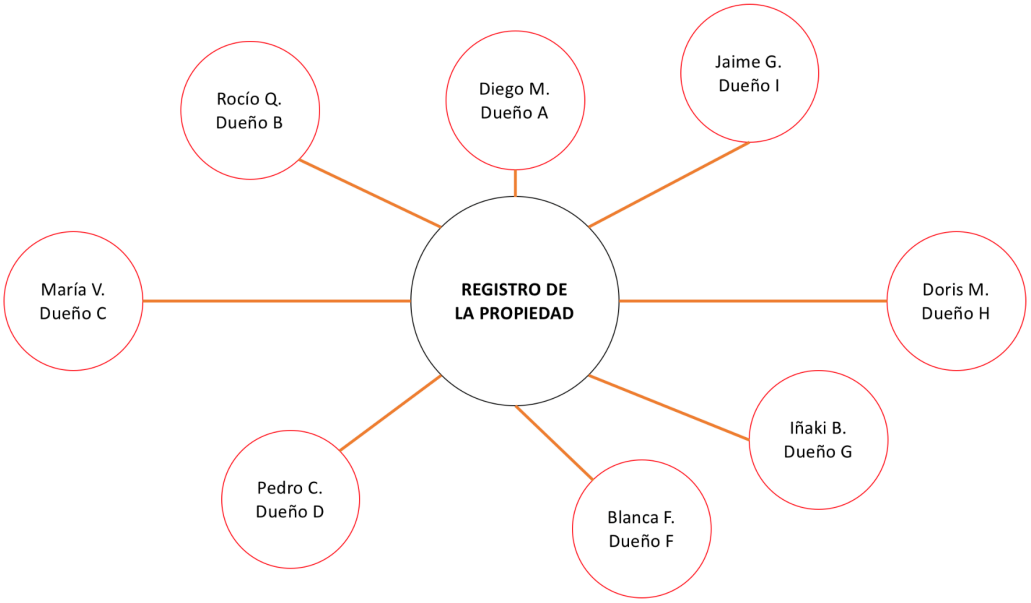
Podemos ver las características esenciales que necesita una *blockchain* para poder mejorar la transparencia de una la ONG Aldeas Infantiles, que lleva ya varios años en funcionamiento, creando valor a sus donantes y, por ello, cumplir mejor sus objetivos.

5.2.- Proyecto de registro público basado en la *blockchain*

Otro problema habitual en países con poca seguridad jurídica es la falta fiabilidad de los registros públicos. Es habitual que en países de Centro América los registros públicos de los inmuebles se alteren en periodos de estabilidad y, cuando se alcanzan épocas de más estabilidad, hay personas que no pueden volver a sus hogares ya que las personas beneficiadas por el conflicto han alterado los datos.

En este caso, el registro público funciona de la manera clásica de ente de confianza. El problema es la falta de confianza en determinados momentos de dicho registro.

FIGURA XII: REGISTRO DE LA PROPIEDAD CENTRALIZADO



Fuente: Elaboración propia

En este caso, cualquiera de los actores podría alterar el registro en las situaciones de inestabilidad y no habría forma de comprobar lo que ha ocurrido.

La aplicación de la *blockchain* daría la seguridad en el largo plazo empleada. Por mucho que se puedan dar situaciones de inestabilidad, en caso de que a continuación se vuelva a una situación democrática donde los derechos tienen que ser respetados, siempre que los nodos y la red se mantenga viva, el registro se podrá mantener.

5.3.- Siembra de campos en zonas desfavorecidas

En la entrevista realizada a Alfonso Masoliver Sagardoy me contó que en su última visita a Guinea-Bissau de junio a mediados de agosto de 2017, una de las cosas que más le impactó es la dejadez de alguno de los trabajos que la ONG había realizado en años anteriores. Tal era el punto que, en los proyectos de plantación de una huerta, lo habitual era dejar a una persona pagada por la ONG que se encargase de mantener los cultivos de la huerta y que la gente de la zona trabajase en la misma, ya que si no dejaban que la selva se volviese a comer el terreno.

Este método acaba siendo poco eficiente ya que, si se quiere que las inversiones realizadas en las huertas (cuando nos referimos a huerta, es una gran plantación de

hectáreas) sean rentables, hay que mantener a una persona la que tiene que trabajar en la misma.

Por medio de la *blockchain*, combinado con otras actividades de las que se hablará posteriormente, se puede mejorar la eficiencia, aportando valor al proyecto:

En primer lugar, la opción de vincular al donante en las actividades realizadas, de igual manera que en el ejemplo de "Aldeas Infantiles". Ello permitiría a las personas que quieren participar activamente en la actividad de la empresa ver cómo sucede y, en este caso se podrías dar una vuelta más sobre su participación.

El donante de la ONG podría llegar a fijar democráticamente junto con los demás participantes en el proceso y la propia ONG cuál es el salario que deba recibir el trabajador, en función de su rendimiento y las circunstancias.

De esta manera se puede alcanzar unos mayores niveles de eficiencia, por un lado, y de control por otro. Con el método actual se cuenta con un equipo de trabajadores cuyos resultados dependen de su buena fe. La *blockchain*, sin embargo, iría recogiendo los datos de las huertas que el trabajador controla (por medio de una foto, empleando la geolocalización y el tiempo en el que se hacen la foto para comprobar que no se cometa ningún error o fraude…) y los distintos nodos podrían ver esta información, con la tranquilidad de saber que es verdad lo recogido en la cadena de bloques. Posteriormente entre los donantes y la ONG se puede fijar cuál es el salario por las actividades realizadas; se determinaría por medio del método de prueba de participación, es decir, en función de la cantidad de dinero aportado por los integrantes de la cadena de bloques (generalmente, la ONG será la que mayor peso tenga, pero también habría que crear medidas de representación significativa de la ONG en la participación a la hora de cerrar un bloque).

De esta manera se ganaría no solo en transparencia y financiación como se ha explicado en el primer ejemplo, si no que *blockchain* da una verdadera fuente de incentivo a los trabajadores, que podrán mejorar la eficiencia y su rendimiento, así como su motivación personal.

Me gustaría mencionar en este punto una de las conversaciones que tuve con Manuel Hurtado sobre este problema en concreto. Con una visión muy amplia, cree que hay

formas de hacer esto aún más eficiente a través del empleo de los nuevos avances tecnológicos; en este caso, era partidario de emplear drones que pudiesen hacer al día varios viajes para comprobar el estado de las plantaciones y subir las fotos obtenidas por los mismos, pudiendo cubrir un trabajador más plantaciones y convirtiéndolo en un proceso aún más eficiente.

5.4.- Creación de un proyecto propio

Otra alternativa, sería crear proyectos solidarios a partir de una plataforma *blockchain*. Pongamos un ejemplo muy concreto: el caso de la educación y el impulso de zonas desfavorecidos.

Planteamiento

El proyecto estaría inicialmente formado por: un impulsor de la idea y una persona o grupo de voluntarios en la zona de acción. Lo que se busca es que la juventud de la zona vaya mejorando su calidad de vida, apoyados por medio del trabajo inicial de unos voluntarios o gente de la zona, en caso de ser estos últimos suficientes.

Desarrollo del proyecto

El fundador del proyecto tendría que definir los objetivos: las personas a ser ayudadas van a tener que cumplir con unos objetivos académicos (que pueden ser desde ir a clase a sacar determinadas notas; se puede establecer niveles en función del tiempo y el punto de partida) y personales (ayudar en las tareas domésticas o cuidar a familiares necesitados).

Paralelamente, cuentan con un padrino (los voluntarios presentes en la zona) que se encargan de controlar sus actividades y suministrarleslos recursos que necesiten. Estos recibirían (en función de si son voluntarios puros o gente de la zona que lo quiere hacer como trabajo para poder salir adelante) una remuneración por su trabajo.

A medida que los ayudados vayan creciendo y cumpliendo fases, se encargarán de cubrir tareas que hacían los propios voluntarios, recibiendo una remuneración por ello

Por su parte, los donantes tienen un contacto con los ayudados a través de las personas de la zona: un donante podrá tener de referencia a un voluntario que controlaría a varios jóvenes de los que se encargaría de empujar. Además de poder ver

como están evolucionando las personas a las que ayudan, también tendrán la opción de participar activamente en el control de sus fondos decidiendo el salario de sus voluntarios; en función del desempeño de los padrinos a los que dan fondos, se crearían niveles de voluntarios y niveles de donantes, relacionándose los voluntarios más productivos con los donantes que tuviesen una participación más pasiva y se asignaría voluntarios nuevos de la zona o "más problemáticos" a aquellos donantes que tenga una inversión más activa en el proyecto y un interés en que salga ganando la totalidad del proyecto (voluntarios y ayudados).

Empleo de tecnología *blockchain*.

Como podemos ver se trata de un plan que requiere una gran inversión de capital humano y de tiempo. Sin embargo, la *blockchain* nos da la oportunidad de ordenar el proyecto de manera que se ahorre mucho por las partes y donde el trabajo está distribuido entre las distintas personas.

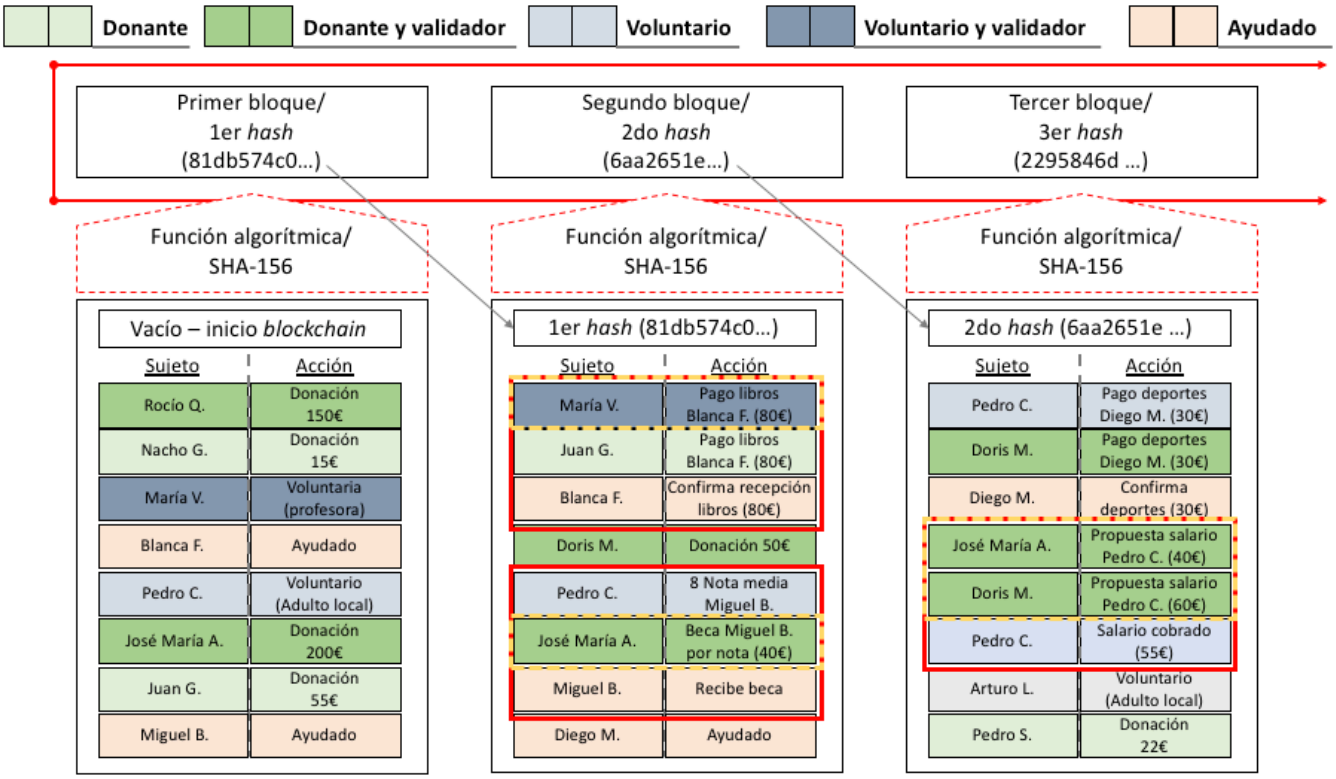
En primer lugar, hay que definir qué tipos de nodos existen:

1. **Nodos donantes**: Son aquellos que donan su dinero con la confianza de que este será bien empleado. A pesar de su rol más pasivo, formarían parte de la red para ayudar a la resiliencia de la misma y poder recibir la información que esta en la misma.
2. **Nodos donantes y validadores**: estas son las personas que aportan los fondos al proyecto y que aprueban las decisiones realizadas ya que quieren tener una verdadera función activa. Son los primeros que tienen el interés de que su dinero sea debidamente empleado.
3. **Nodos voluntarios**: Serían todas las personas que trabajan en la zona desfavorecida para poder desarrollar el proyecto.
4. **Nodos voluntarios y validadores**: son aquellos nodos voluntarios que se han ganado la confianza de la gente que forma parte de la red. Esta confianza se puede conseguir por los resultados obtenidos con las personas ayudadas y la opinión de los donantes de los que lleva sus fondos.

5. **Nodos ayudados**: Serían las personas últimas que reciben la ayuda. No solo están para mejorar la resiliencia de la red, si no que serían necesarios para poder ratificar algunas de las operaciones realizadas.

De esta manera, los nodos que formarían parte a la hora de fijar un bloque son aquellos que tienen un especial interés en el correcto funcionamiento: los voluntarios en los que se puede confiar (como podrían ser los profesores de la escuela de la zona) y los donantes que tiene una participación activa. Aunque el método es, efectivamente, el de prueba de participación, no se hace en función de la cantidad donada, si no en función del número de actividades en las que se encuentre presente el nodo validador que dependerá para los voluntarios, en función de la confianza adquirida y, para los donantes, una mezcla de confianza y cantidad donada.

FIGURA XIII: PROGRAMACIÓN *BLOCKCHAIN* PROYECTO PROPIO



Fuente: Elaboración propia

En la figura XII se puede ver cómo sería el funcionamiento dentro de la *blockchain.*

Por un lado, las operaciones que se van realizando dentro de la misma tienen que tener un nodo validador presente: así, en el caso del segundo bloque, María V.,

profesora del colegio y voluntaria de confianza se encarga de confirmar la operación realizada. En la otra operación, el validador no sería el voluntario, sino el donante (José María A.) que tiene un rol activo en el control de sus fondos y que ayuda a la ONG en funciones de control, incluso de los voluntarios que están dando sus primeros pasos. Podría darse la situación de que alguno de los entes validadores actuase de mala fe, pero esto atentaría contra su propio interés, al perjudicar su imagen y llevar implícita una sanción.

En cuanto a la decisión de un método democrático para decidir el salario de los voluntarios se puede ver en el ejemplo del tercer bloque sobre cómo se determina el salario de Pedro C., el cual ha realizado operaciones con José María A. y con Doris M. Ambos dicen que salario consideran óptimo y automáticamente se hace una media de las propuestas que saldaría su salario en función de la conformidad del donante (en este caso, se ha fijado un salario mínimo de 50 euros que es con el que se hace media en vez de la propuesta de 40€ de José María A., para mantener así cierta justicia al trabajo realizado y donantes que quieran que todo su dinero vaya destinado solo a la obra social encuentren un freno, en aras del carácter retributivo y de continuidad del proyecto).

A estas formas de comprobación se les podría añadir otras como la geolocalización de las personas involucradas en momentos concretos (por ejemplo, si lo que se le pide a un ayudado es que acuda a todas las clases, una geolocalización de su móvil favorece para saber dónde estaba y en qué momento); también cabe ir ampliando la red a otros actores que pueden tener relevancia: la tienda donde se compran los materiales para los alumnos, la policía local, miembros de la zona que quieran colaborar…

Como conclusión, se puede ver como la creación de una *blockchain* como base de la operativa de una ONG tiene cuatro consecuencias principales:

1. Facilita las vías de financiación de la entidad gracias a las microdonaciones y una transparencia y seguridad difíciles de superar
2. Permite una mayor transparencia funcional, estando conectados en todo momento la actividad de la ONG y la fuente de su financiación.
3. Da la opción de que los trabajadores de la ONG tengan los incentivos para mejorar su trabajo, más allá del bien social que consiguen

4. Aporta a todas las operaciones realizadas una gran seguridad en el tiempo. Evidentemente con la *blockchain* no se eliminan las acciones fraudulentas, pero sí que se consigue una transparencia total en caso de que se cometa tanto una acción contraria al fin social o se pretenda ocultar algo hecho en el pasado.

5.5.- Problemas en la implementación de todos los proyectos.

Como bien explicaron José Luis Gahete Díaz, David Contreras Bárcena e Israel Alonso Martínez, hay que prestar atención con el desarrollo de los proyectos *blockchain* ya que hay una percepción de que lo puede cambiar todo, pero al hablar de todo se acaba por no concretar en nada.

En este apartado se pretende exponer las partes en las que cojean los distintos casos creados:

En primer lugar, los costes: en todos los apartados mostramos las virtudes de una *blockchain.* Sin embargo, hay que saber que el desarrollo de una tecnología como esta exige ciertos recursos y que la cantidad de programadores disponibles no es muy alta. Por tanto, es muy importante realizar una buena elección del equipo y concretar las ideas para que se pueda implementar rápidamente y escalable con facilidad (Daniel Díaz García veía fundamentales estos dos puntos a la hora de emprender algo con tecnología *blockchain*).

También es importante tener en cuenta que la gran mayoría de las soluciones previstas se podrían dar al margen de la *blockchain*, pero es importante recordar que lo que se pretende no es solucionar por completo un problema (ya que eso es imposible; siempre habrá maneras de engañar al sistema), sino mejorar la eficiencia y funcionalidad de los principales retos a los que se enfrentan los proyectos de las ONGs. Aunque se podría reducir la aplicación de la *blockchain* a que solo aporta seguridad en el largo plazo, se estaría ante una opinión limitada.

Otro punto débil es el tamaño de la *blockchain:* a mayor cantidad de nodos y de bloques hace que la red sea más infranqueable que una cadena de pocos años y pocos

nodos. Hay que tener en cuenta que en muchos de estos casos, la cadena de bloques comenzará con muy pocos nodos.

Por último, en todos los casos se habla de la creación de nodos. Es muy importante tener en cuenta que la *blockchain* no se trata de una base de datos, sino que es un protocolo fiable en una arquitectura distribuida; esto implica que los nodos no son un nuevo asiento en la base de datos, si no verdaderas unidades computacionales que necesitan de representación física y un sistema operativo que le permita participar en la red. Esto sería un inconveniente para el desarrollo de algunas iniciativas, como el caso de Aldeas Infantiles SOS en el que habría que profundizar sobre cómo convertir a los donantes en nodos.

6.- Conclusión

En el presente trabajo se ha buscado ver qué maneras prácticas podía la *blockchain* ser empleada en proyectos solidarios. Al principio de la investigación sabíamos que era una tecnología que aportaba seguridad y transparencia al aplicarla y que eliminaba el doble gasto. Por otro lado, esta el mundo del tercer sector, donde la confianza juega un papel clave y los fallos en facetas como la transparencia, la seguridad o el empleo de los fondos, pueden dañar gravemente su imagen, llegando incluso a poder provocar su extinción.

De la primera hemos aprendido su amplia gama de programación, que permite preparar el funcionamiento de la *blockchain* para todo tipo de situación. Se trata de un protocolo fiable estructurado en una arquitectura de capas distribuidas (*DTL*). A la seguridad y transparencia, se le añade la flexibilidad para adaptarse a los diferentes proyectos y la compatibilidad con otras tecnologías que permite llegar a un bien conjunto en el desarrollo de proyectos.

Respecto a las actividades del tercer sector, se sabe que tienen que ser entes autónomos, que puedan subsistir por sí mismo y que precisan del trabajo de los voluntariados. Tienen que ser innovadores, prestar servicios a los grupos en necesidad, intermediarios y defensores de los protegidos.

Los principales problemas que se han identificado son: la transparencia, tanto funcional como financiera, la aportación de valor, las condiciones laborales y la ejecución de los planes estratégicos. Los tres primeros, si bien no solucionados, si que pueden mejorarse aplicando la tecnología *blockchain.*

Una vez localizadas, se han propuesto un conjunto de ejemplos en los que se ven las flaquezas en esas facetas y una propuesta práctica de solución con la *blockchain:*

El primer ejemplo ha sido el caso de Aldeas Infantiles SOS. Es un proyecto solidario de ayuda a jóvenes sin familia que tiene problemas de transparencia funcional y financiera. Su actividad hace necesario precisamente mantener dicha discreción. Por medio de la *blockchain* se consigue crear un método de vinculación de los fondos a las actividades realizadas. La *blockchain* estaría basada en las personas que realizan las

donaciones, con la información de sus fondos en la ONG y tendrían una función validadora de la mano de la organización central de Aldeas Infantiles, que a la hora de determinar las operaciones tendrá un peso determinante. De esta manera, el donante no solo sabrá que sus fondos están llegando a buen puerto, si no que también sabrá donde concretamente y podría crear una fidelidad de donación con la ONG.

El segundo ejemplo, sería un caso de aportar valor. El problema expuesto es la situación de un registro público centralizado que en periodo de inestabilidad queda alterado y no existe la seguridad jurídica. En este caso, la *blockchain* aporta valor *per se* permitiendo fijar el registro sin necesidad de un ente central de "confianza" que ante las desestabilidades sociales puede ser modificado sin proteger a las personas afectadas. En caso de que haya inestabilidad y se realizasen cambios, la *blockchain* misma pondría de manifiesto la alteración y cuando se volviese a la normalidad, los ciudadanos pueden ejercer sus derechos.

El tercer caso es una combinación de proyecto que aportar valor y controlar la gestión de los trabajadores en la zona. La *blockchain* se programa para aceptar una serie de datos que corroboren que se están cumplimiento los objetivos. Además, se pretende poder tener un mayor control sobre la eficiencia del trabajador que resultaría en dos cosas: por un lado, disminuir costes al reducir el número de la plantilla y, por otro, mejorar el salario de aquellos trabajadores que hagan una actividad más eficiente.

Finalmente, se expone un caso que engloba todos los puntos anteriores. El objetivo es configurar un proyecto solidario para ayudar a barrios desfavorecidos y a sus jóvenes. El proyecto se estructura en torno a una *blockchain* formada por cinco tipos de nodos: los donantes involucrados y validadores, los donantes pasivos, los voluntarios de confianza y validadores, los voluntarios y las personas ayudadas. El objetivo consiste en crear una estructura de méritos que da distintas responsabilidades a los nodos (siendo los validadores los que tengan el principal interés del correcto funcionamiento), manteniendo informado en todo momento a los inversores y participando los mismos en el pago de los voluntarios que formen parte del proyecto.

Concluyendo, se puede ver como la tecnología *blockchain* es una opción para solucionar los principales problemas a los que se enfrentan los proyectos solidarios,

pero hay que ser conscientes de los problemas de la implementación de estos proyectos como podrían ser coste de la programación o tamaño de la cadena de bloques.

Bibliografía

ACNUR Comité Español, ¿Qué es una ONG y cuál es su función social? Obtenida el 27/2/2018 de https://eacnur.org/blog/una-ong-funcion-social/

Aldeas Infantiles. Conócenos. Misión. Obtenida el 30/03/3018 de https://www.aldeasinfantiles.es/mision

Asociación española del *fundraising.* (2016). *Perfil del donante.* Obtenida el 20/02/208 de https://www.aefundraising.org/wp-content/uploads/2017/09/Perfil_donante-2016-_-resumen-ejecutivo.pdf

Buterin, V. (2014) Slasher: A punitive proof-of-stake algorithm. Ethereum blog. Obtenida el 10/03/2018 de https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

Buterin, V. (2016) A proof of stake design philosophy. Medium. Obtenida el 4/03/2018 de https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

Buterin, V. (2017) Proof of Stake FAQ. Obtenida el 29/03/2018 de https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

Cabra de Luna, M.A (1998), *El Tercer Sector y las Fundaciones de España hacia el nuevo Milenio*, Madrid: Escuela Libre

Drescher, D. (2017). Reinventing the Blockchain. *En Blockchain Basics* (pp. 213-220). Apress.

El Eonomista. (2018). La crisis de Oxfam lleva a otras ONG a ocultar escándalos para evitar castigos. Obtenida de http://www.eleconomista.es/internacional-eleconomista/noticias/8937443/02/18/La-crisis-de-Oxfam-lleva-a-otras-ONG-a-ocultar-escandalos-para-evitar-represalias.html

Europa Press. (3/3/2018). La ONG 'it.willbe.org' utiliza la tecnología de IBM blockchain para aumentar la confianza de los donantes. La vanguardia. (Obtenida el 18/02/2018 de http://www.lavanguardia.com/vida/20180313/441504378946/la-ong-

itwillbeorg-utiliza-la-tecnologia-de-ibm-blockchain-para-aumentar-la-confianza-de-los-donantes.html)

Fernández. C. (2018). IBM explota la aplicación de blockchain en ONGs de la mano de la organización española it-willbe. *Criptonoticias.* (Obtenida el 14/03/2018 de https://www.criptonoticias.com/adopcion/ibm-explora-aplicacion-blockchain-ongs-mano-organizacion-espanola-it-willbe/)

Hurtado M. (13/3/2018a) Blockchain para incrementar la confianza en la solidaridad. *El Pais.* (Obtenido el 14/3/2018 de https://retina.elpais.com/retina/2018/03/13/tendencias/1520932308_667890.html)

Hurtado M. (2018b) Blockchain aporta a los donantes confianza en las ONGs. *IBM Think España*. (Obtenido el 14/3/2018 de https://www.ibm.com/blogs/think/es-es/2018/03/13/blockchain-aporta-confianza-en-las-ongs/)

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review*, 95(1), 118-127.

Izquierdo, B. G. (1999). Análisis del sector de las ONGD españolas: fortalezas, debilidades y retos. *Boletín de Estudios Económicos*, 54, 557.

Jimenez Lara, A. (2006) El mosaico no lucrativo*.* En Ruíz Olabuenaga, J. (Dir), *El sector no lucrativo en España, una visión reciente* (27-85)*,* Madrid: fundación BBV

Lage Serrano, O. (2017) Participación ciudadana y voto electrónico*.* En Preukschat, A. (coordinador). *Blockchain, la revolución industrial de Internet* (100-102) Madrid: Grupo Planeta.

Moro, L. (dir) (2009). *Gestión actual de una ONG.* LID, Madrid

Nakamoto, S. (2008). Bitcoin, a peert-to-peero electronic cash system. Obtenido el 15/1/2018 de www.bitcoin.org/bitcoin.pdf

Navajo P. (2009). Dirección estratégica*.* En Moro, L. (dir) (2009). *Gestión actual de una ONG* (107-143). LID, Madrid

Núnez Miller, J. (2017). Criptografía y consenso aplicado a la blockchain. En Preukschat, A. (coordinador). *Blockchain, la revolución industrial de Internet* (203-219). Madrid: Grupo Planeta.

O'neill, S. (2018). Top Oxfam staff paid Haiti survivors for sex. *The times*, Nº 72453, UK.

Preukschat A. (coordinador). (2017*). Blockchain, la revolución industrial de Internet*. Madrid: Grupo Planeta.

Santos, B. (20/2/2018). Blockchain, innovación para el desarrollo y el sector social. *El país. (Obtenido el 27/02/2018 de https://elpais.com/elpais/2018/02/20/3500_millones/1519135197_223333.html?id_externo_rsoc=whatsapp)*

Servula B. (6/10/2017). El blockchain es la tecnología más disruptiva que va a haber en el mundo de Internet. *El economista.* (Obtenido el 15/02/2018 de http://www.eleconomista.es/negocio-digital/noticias/8656964/10/17/El-blockchain-es-la-tecnologia-mas-disruptiva-que-va-a-haber-en-el-mundo-de-Internet.html)

Tapscott D, Tapscott, A. (2016). *La revolución blockchain, descubre como esta nueva teconología transformará la econmía global*. Trad. J. M. Salmerón. Barcelona: Deusto

Ruíz Olabuenaga, J., 2000, *El sector no lucrativo en España*, Madrid: fundación BBV.

Ruíz Olabuenaga, J. (Dir), 2006, *El sector no lucrativo en España, una visión reciente,* Madrid: fundación BBV.

Salas A. (2009). El tercer sector en España. En Moro, L. (dir) (2009). *Gestión actual de una ONG* (29-41). LID, Madrid

Szabo, D. (1997). *The God Protocol*. Obtenida el 15/03/2018 de http://nakamotoinstitute.org/the-god-protocols/

Vernis, A. (dir), (2004), *Los retos en la gestión de las organizaciones no lucrativas, claves para el fortalecimiento institucional del tercer sector,* Madrid: Ediciones Granica

Glosario de términos

Alastria	Consorcio de empresas españolas que ha creado la primera blockchain semipública permisionada
DLT	*Distributed Ledger Technology*
Hash	Combinación alfanumérica resultado de aplicar la función algorítmica SHA-265
Nounce	Combinación de números y letras que se introduce junto con la información y el hash del anterior bloque para conseguir que se cumple el requisito del método de prueba de trabajo
Peer to peer	De usuario a usuario
Remuneración psicológica	Forma de denominar a la remuneración no monetaria pero que satisface personalmente al trabajador
Smart Contract	Contratos programables que se ejecutan automáticamente si se cumplen las situaciones previamente fijadas